بحث بعنوان

أمن المعلومات في البيئة الإلكترونية

(دراسة قانونية لدراسة مفهوم أمن المعلومات والمواجهة القانونية الجنائية)

من إعداد الباحث

عقيد دكتور/ أيمن سيد محمد مصطفى

ت/ ٠١٢٧٠٥٢٢٢٥-٠١٢٢٥٢١١١٢٢

بسم الله الرحمن الرحيم

(يا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ ۖ وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا ۚ أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ ۚ وَاتَّقُوا اللَّهَ ۚ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ)

(الحجرات ١٢)

مقدمة

لم يكن بمقدور العالم أن يتخيل أبدا أن العلم سيحقق انجازات تختصر الزمان والمكان من خلال وسائل الاتصال والتي جعلت من العالم من خلال قاراته وبلدانه ما هو إلا قرية صغيرة ، وقد دخلت الأقمار الاصطناعية على خد الاتصالات على نحو أدى إلى ظهور طفرة نوعية وكمية في حجم الاتصالات .

صاحب ذلك التطور ظهور الحاسب الآلي الذي بدوره تطور تطورا غير مسبوق وبشكل متسارع ليقدم علم الإليكترونيات ، وهذا ما نتج عنه تطور في استخدام الحاسوب وتطبيقاته ، وبظهور شبكة الإنترنت كوسيلة اتصالات عالمية ساهمت في تقارب الشعوب والثقافات ([1])، وما زاد من قيمتها ظهور الهاتف المحمول وما صاحبه من تطور وبخاصة متى كان مرتبطا بالإنترنت.

هذا التطور السريع في تقنيات الاتصال الحديثة أدى إلى دخول العالم في عصر تم تسميته بعصر المعلومات أو الثورة المعلوماتية ، أو تقنية المعلومات (**Telecommunication**)وغيرها من التسميات والتعبيرات التي تحمل نفس المعنى ، فقد انسابت المعلومات من كافة مصادرها سواء عن طريقها أو بواسطتها ، ونظرا لالتفاف الأشخاص والجماعات والدول حولها من مختلف البلدان والقارات والأجناس.

وفعلت هذه التقنية ما لم تفعله السياسة في توحيد الشعوب والثقافات ، وعلى الرغم من المزايا المكتسبة من التطور في تقنية المعلومات في شتى المجالات والميادين إلا أن هذا التطور في ذات الوقت حمل معه بذورا للشر التي كان تنتظر من يسقيها مياه الحياة ، وسرعان ما وجدت ساقيها والذي تمثل في المجرم الذي يتصف بميزات وسمات تميزه عن غيره من المجرمين العاديين هو ما تم تسميته بالمجرم الإليكتروني .

هذا الأخير وجد ضالته التي كان يبحث عنها في تلك التقنية الحديثة للمعلومات والتي أتاحت له فرصة ارتكاب الجريمة والحصول من ورائها على اكبر قدر من النتائج الإجرامية التي

---

[1] – هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات،مكتبة الآلات الحديثة،أسيوط،١٩٩٢،ص٥.

يهدف إليها بأقل قدر من ممكن من الخسائر والمخاطر ، معتمدا في ذلك على ما يملكه من مهارة فنية وتقنية .

وهذه الجرائم تنقسم لقسمين ، الأولى يعد فيها النظام المعلوماتي وسيلة لارتكاب الجريمة ، بينما الطائفة الثانية يكون الضحية فيها هو النظام المعلوماتي ، وهو الأمر الذي جعلناه محورا لبحثنا هذا نظرا للخطورة الشديدة الناجمة على الاعتداء على النظام المعلوماتي في ظل تزايد الاعتماد على النظام المعلوماتي في شتى مناحي الحياة سواء العامة أو الشخصية ، وما كبده الاعتداء على النظام المعلوماتي من خسائر جمة سواء مادية أو معنوية نظرا لسهولة ارتكاب هذه الجريمة بالإضافة أنها جريمة عابرة للحدود يصعب تعقب المجرم واكتشافه وتحديده نظرا لما يتميز به المجرم المعلوماتي من ذكاء وتقنية ، بالإضافة إلى الطبيعة المتميزة لمحل الاعتداء والمتمثل في المعلومات المتواجدة في البيئة المتميزة.

أهمية البحث :-

تعود أهمية أمن المعلومات اليوم إلى عاملين مهمين أولهما هو الاعتماد الكبير للمجتمعات اليوم على المعلومات ووسائطها في الاتصال والتجارة والكثير من الأنشطة، والثاني أن منظومات المعلومات اليوم تدير معظم النشاط البشري في قطاع الخدمات والأعمال والاتصال على مدار الساعة. ومن هنا فإن أي إضرار بهذه المنظومة العالمية للمعلومات ستؤثر بلا شك في حياة المجتمعات وراحتها بشكل مباشر..

حيث أنه يقع على المشرع واجب كبير في هذه المرحلة و هو مواكبة عصر العولمة و عصر الرقمنة و يغير من المفاهيم السائدة التي تعتبر تقليدية بالنسبة لهذا العصر ، و ذلك بأن يعدل المشرع نصوصه القانونية المتوفرة لتتماشى مع مستجدات هذا العصر ، كما عليه أن يستحدث منظومة قانونية تماشيا مع المتطلبات الواقعية و المستقبلية

أهداف البحث:-

تتمثل أهداف البحث في النقاط الآتية :-

- دراسة المشكلات التي تواجه دراسة أمن المعلومات في بيئة الأعمال الإليكترونية باعتبارها نمطا مستحدثا من أنماط الجرائم ، وهي الجريمة المعلوماتية وبخاصة الاعتداءات الواقعة على النظام المعلوماتي.

- من خلال الجانب الإجرائي فيما يخص الدليل التقني نبين مفهومه ومشروعيته ومصداقيته الثبوتية ومختلف الإجراءات التقليدية والمستحدثة التي تخص البحث عن أدلة الاتهام ، وملائمة تلك الإجراءات لمواجهة الخطورة الإجرامية لمختلف السلوكيات المهددة لأمن المعلومات الإليكترونية.
- عجز النصوص التقليدية للتعامل مع تلك الجرائم والتي كانت سببا لتكريس قواعد قانونية خاصة بأمن النظام المعلوماتي من الاعتداءات الواقعة عليه.
- تحديد جوانب القوة والضعف في المعالجة التشريعية لجرائم الاعتداء على النظام المعلوماتي ، وسد الثغرات القانونية التي يستغلها المجرم للإفلات من العقاب.

إشكاليات الدراسة :-

ترجع إشكاليات البحث إلى ما يتميز به من صفة فنية ، ومفردات ومصطلحات جديدة كالبرامج والبيانات التي تشكل محلا للاعتداء أو تستخدم كوسيلة للاعتداء ، معظم مستندات موضوعه (الجريمة الإلكترونية) عبارة عن تسجيلات إلكترونية تتم عبر شبكات الاتصال المعلوماتي ، ذات طبيعة خاصة متميزة ، وذلك راجع إلى عدة عوامل منها طبيعة المال المعلوماتي وحداثة ظهور الحاسب الآلي وتقنية تشغيله ، ولهذا أصبح لا يكفي أن يكون الباحث متخصصا في القانون ، بل يتعين عليه أن يكون ملما بالجوانب الفنية للحاسب الآلي والإنترنت ليتمكن من إيجاد الحلول للتحديات والمشاكل القانونية التي تثيرها شبكة الاتصال والمعلومات و جرائمها الإلكترونية ، كما أن عدم وجود قانون يجرم التقنيات الفنية الجديدة الناشئة عن استخدام الانترنت في ارتكاب الجرائم التقليدية أدى إلى اللجوء إلى التفسير ، الأمر الذي أثار إشكاليات التكييف القانوني للفعل كما يثير مشكلة التمييز بين العمل التحضيري والبدء في تنفيذ الجريمة وغيرها، كما أن التعامل مع دليل هذا النمط من الجرائم فتح مجالا جديدا في الإثبات ، فبعد أن كان مجال الإثبات ينحصر فقط في المستند الورقي أصبح الدليل الرقمي

ينازعه في هذه المرتبة ، ناهيك عن وجود بعض الصعوبات العملية في تطبيق الأفكار التقليدية والمستقرة بالقانون الجنائي كمبدأ الشرعية وسريان القانون من حيث الزمان والمكان واختصاص القضاء الوطني .

تساؤلات الدراسة :-

- ماهية أمن المعلومات والتحديات التي يواجهها؟
- ماهية تصنيفات وأساليب التهديدات لأمن المعلومات في البيئة الإليكترونية ؟
- ماهية الاتجاهات القانونية والتقنية لمواجهة الاعتداءات على أمن المعلومات
- مدى ملائمة المواجهة التشريعية والإجرائية لموجهه الاعتداءات على أمن وسلامة المعلومات في البيئة الإليكترونية؟

الدراسات السابقة :-

من الدراسات ذات الصلة بذات الموضوع الدراسات الآتية :-

- محمد الدسوقي دراسة بعنوان الحماية الجنائية لسرية المعلومات ، دار الكتب القانونية ،مصر ،٢٠٠٣.
- نهلا عبد القادر المومني ، الجرائم المعلوماتية ، دار الثقافة ، ط١ ، عمان الإصدار السادس ٢٠١٠م
- عبد الله قاسم حميد ، الحماية الجنائية للمعلومات الإليكترونية ، رسالة ماجستير ، جامعة عين شمس ، القاهرة ،٢٠١٠.

المنهج المستخدم :-

المنهج الوصفي الذي يصف الظاهرة بتحليلها لجزئيات ندرسها و نتعمق فيها لنفهم أصل الظاهرة و حقيقتها العلمية و القانونية.

المنهج المقارن و الذي من خلاله نقارن التشريع المصري بالتشريعات المقارنة بالخصوص الفرنسي والأمريكي بجانب العربية ، هذا بالإضافة إلى الاتفاقيات الدولية ذات الصلة بموضوع الدراسة.

المنهج التحليلي و هذا من خلال تحليل الإستراتيجية التشريعية المنتهجة لتوفير الحماية للمعلومات الإلكترونية

تقسيم الدراسة :- من أجل تحقيق المبتغي من هذه الدراسة رأينا تقسيمها على النحو التالي:-

المبحث الأول :- ماهية أمن المعلومات والتحديات التي يواجهها وينقسم إلى :-

المطلب الأول :- مفهوم أمن المعلومات

المطلب الثاني :- التحديات والتهديدات التي تواجه أمن المعلومات في البيئة الاليكترونية

المطلب الثالث :- تصنيفات وأساليب التهديدات الأمنية لأمن المعلومات

المبحث الثاني:- المواجهة التقنية والتشريعية لحماية أمن المعلومات وإشكاليا ته

المطلب الأول :-المواجهة التقنية لحماية أمن المعلومات والمعوقات التطبيقية لذلك

المطلب الثاني :-الاتجاهات التشريعية لأمن المعلومات من الاعتداءات عليه

المطلب الثالث :- الإطار القانوني الدولي والوطني لمواجهة جرائم الاعتداء على أمن المعلومات.

المطلب الرابع :- مدى ملائمة المواجهة التشريعية لمواجهة الاعتداءات على أمن المعلومات

المبحث الأول

ماهية أمن المعلومات والتحديات التي يواجهها

عرف أمن المعلومات بأنّه أحد فروع العلم الباحث في مجال توفير الحماية اللازمة للمعلومات ومنع الوصول إليها وهدرها من غير ذوي الصلاحية، وحمايتها من أيّ تهديد خارجي، ويشمل هذا المصطلح الأدوات والطرق والإجراءات اللازمة الواجب توفرّها لتحقيق الحماية

ويُعتبر هذا العلم نوعاً من تمكين المستخدم فرض سيطرته على المعلومات بشكل كامل، ومنع الآخرين من الاطلاع عليها أو إجراء أي تغيير عليها دون إذن مسبق، فإذن أمن المعلومات هي عبارة عن حزمة من العمليات والطرق والإجراءات يتمّ انتهاجها من قبل بعض القطاعات ومنظّمات التأمين لبسط أقوى طرق الحماية على المعلومات الخاصة بها وعلى أنظمتها ووسائطها لمنع الوصول إليها لغير المصرّح لهم بذلك.

تمتاز حماية المعلومات بأنها مستمرة، أي إنها تحتاج بالضرورة إلى الاستمرارية في مواكبة كل ما هو مستحدث ومتطور من درجات الأمان وأساليبها في حماية هذه المعلومات، كما تتطلّب الاستمرارية بفرض الرقابة على المخاطر وافتراضها، والسعي الدائم لإيجاد حلول وابتكارات دائمة، ولذا لا يطلق النظام المعلوماتي الأمني الحقيقي على نظام أيّ مُنظّمة إلا في حال كان فعّالاً ومحققاً للاستمرارية في مواكبة العمليات الأمنية والتقنية سعياً للوصول إلى أقل فرصةٍ من المخاطر التي من الممكن تواجه المعلومات الخاصة بها،وتنقسم دراستنا لهذا المبحث لتكون علي النحو التالي :-

المبحث الأول :- ماهية أمن المعلومات والتحديات التي يواجهها وينقسم إلى :-

المطلب الأول :- مفهوم أمن المعلومات

المطلب الثاني :- التحديات والتهديدات التي تواجه أمن المعلومات في البيئة الاليكترونية

المطلب الثالث :- تصنيفات وأساليب التهديدات الأمنية لأمن المعلومات

المطلب الأول

مفهوم أمن المعلومات

مفهوم أمن المعلومات Security Information لقد اختلفت المفاهيم التي أوردها الباحثون بشأن تحديد مفهوم لأمن المعلومات وفيما يأتي بعض المفاهيم كما وردت في كتابات عدد من الباحثين يقصد بأمن المعلومات حماية وتأمين الموارد المستخدمة كافة في معالجة المعلومات ،إذ يكون تامين الشركة نفسها والأفراد العاملين فيها وأجهزة الحاسبات المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات الشركة(٢)

وأيضا أمن المعلومات هو وقاية لسرية، وسلامة المعلومات قانونيا ([٣]) ، في حين عرف امن المعلومات .هو اختصار الطرق والوسائل المعتمدة للسيطرة على أنواع ومصادر المعلومات كافة وحمايتها من السرقة ،والتشويه ,والابتزاز، والتلف، والضياع والتزوير، والاستخدام غير المرخص ،وغير القانوني ([٤])

وكذلك أمن المعلومات يعني كل السياسات والإجراءات والأدوات التقنية التي تستخدم لحماية المعلومات من أشكال الاستخدام غير الشرعي كلها للموارد مثل السرقة ،والتغير ،والتعديل،و إلحاق الضرر بالمعلومات المتعمد([٥])، وهناك من يرى أن أمن المعلومات يتكون من العديد من المكونات ذات المدلول التي تشير إليها علي النحو التالي:-

– فكلمة الأمن تشير إلى طيف واسع من المجالات ضمن وخارج حقل تقنية المعلومات .ويشمل امن المعلومات الخصائص الخمسة الآتية :٢ –السرية ١ –التحقق من الهوية ٣ – الكمال ٤ –التوفير ١ –مكافحة الإنكار (المسؤولية)([٦]) ، فعند ذكر كلمة أمن المعلومات فإن ، ما يتبادر إلى الذهن غالبا هو كشف المعلومات التي كان يجب أن تبقى سرا ،والحقيقة أن

---

[٢] - حسن طاهر داوود ، الحاسب وامن المعلومات ، مركز الدراسات و البحوث ، المملكة العربية السعودية ، ٢٠٠٠م ،ص٢٣.

-3- Micki Krause ; Harold F. Tipton , Information Security Management Hand book , Sixth Edition , Auerbach Publication , New York , 2008[٣]

[٤] – هيثم محمد الزعبي ، إيمان فاضل السامرائي ، نظم المعلومات الإدارية ، الطبعة الأولى ، دار صفاء للنشر والتوزيع ، عمان ، ٢٠٠٤م ص ٢٣٨.

[٥] - سعد غالب ياسين ، نظم المعلومات الإدارية الطبعة العربية ،دار اليازوري العلمية للنشر والتوزيع ، عمان الأردن ،٢٠٠٩ ،ص٣٤٨

[٦] – نجم عبد الله الحميدي ، نظم المعلومات الإدارية مدخل معاصر ، الطبعة الثانية ، دار اليازوري للنشر والتوزيع, عمان ، الأردن ، ٢٠٠٩ م ، ص ١

الحفاظ على المعلومات وسريتها يكون جانبا واحدا من جوانب الأمن ،إذ أن لأمن المعلومات مكونات ثلاثة مكونات على درجة واحدة من الأهمية وهي([٧])

(سرية المعلومات – سلامة المعلومات –ضمان الوصول إلى المعلومات والموارد الحاسوبية وكذلك أنظمة المعلومات متكونة من ثالثة أجزاء رئيسة هي مكونات أمن المعلومات (–السرية –السلامة ٣ –التوفير بغض النظر عن الشكل الذي قد تأخذه المعلومات) الكتروني ،أو مطبوع .

وأشار الزهيري إلى مفهوم أمن المعلومات من عدة زوايا وهي :–

–– زاوية أكاديمية : هو العلم الذي يبحث في نظريات واستراتيجيات توافر الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.

– زاوية تقنية : هي الوسائل والأدوات والإجراءات اللازم توافرها لضمان حماية المعلومات من الإخطار الداخلية والخارجية.

– زاوية قانونية : فان أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوافر المعلومات ،ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة . في حين أن الخوف وعدم الثقة في معاملات الشبكة يمكن التخلص منها عن طريق وضع أنظمة معلومات مؤمنة جديرة بالثقة هذا من جهة . إما من جهة أخرى عن طريق تهيئة اطر تشريعية وقانونية تنظم المعاملات الالكترونية للتأكد من منشأ المعلومة وكمال المعلومة ([٨]) ، فالمعلومات يجب أن تحظى كغيرها من الحقوق بحماية قانونية ولاسيما حماية جنائية تكفل عدم المساس بها وهناك من يرى أمن المعلومات من زوايا تقنية إن استخدام تطبيقات التكنولوجيا وتدابير أمن المعلومات التي يمكن أن تمنع الانتهاكات والاعتداءات داخل المجتمعات والمنظمات أظهرت الحاجة الملحة لاستباقية قوية إلى توافر قيمة علمية كبيرة للباحثين والأكاديميين والممارسين في

---

٧ – محمد بن عبد الله القحطاني ، امن المعلومات ، جامعة الملك عبد العزيز للعلوم والتقنية , الرياض ،٢٠٠٩م ،ص٢٣.

٨ – خالد ممدوح إبراهيم ، امن المعلومات الالكترونية ، الدار الجامعية ، القاهرة ،٢٠٠٨م ، ص٧.

مجال تكنولوجيا المعلومات والأمن .ومن القضايا ذات الصلة مثل مراقبة الموظفين وسياسات أمن المعلومات وصعوبة كلمة المرور([9])

(ومما تقدم نلحظ أن البعض اخذ مفهوم أمن المعلومات من زاوية قانونية وذلك بوجوب وضع التشريعات والقوانين لحماية المعلومات . والبعض الأخر أخذه من زاوية تقنية بوضع الأدوات والوسائل لحماية المعلومات . و لكون امن المعلومات احد عناصر البنية الأساسية التي يجب أن تتاح لأمن نظام المعلومات الخاص بالشركة فعند التخطيط له يجب توازن قيمة المعلومات

لإدارة الشركة مع الحجم النسبي لأنواع المعلومات في مواجهة حد الأمن المتوسط في الأساس. وفي كثير من الشركات والأجهزة الحكومية تتوافر منظومات أمن صارمة لمعالجة وتخزين واسترجاع المعلومات ونقلها بطريقة "تحمي سريتها وسلامتها في مستودعاتها المقروءة آليا.

المطلب الثاني

التحديات والتهديدات التي تواجه أمن المعلومات في البيئة الإليكترونية

أولا :- التحديات الأمنية :-

في الوقت الذي تدخل الإنترنت في شتى مناحي الحياة اليومية أكثر فأكثر ، فإن الأخطار اليومية المتعلقة بالإنترنت تزايدت بشكل غير مسبوق ، فلم يصبح السؤال " هل من الممكن الاختراق " ولكن " متى سيتم الاختراق" ، حيث أن معظم أجهزة الإنترنت تفتقر إلى الأمن والخصوصية الكافية لحماية مستخدميها، وقد كشفت شركة HP أن٧٠% من إنترنت الأشياء تحتوي على ثغرات أمنية يمكن لمرتكبي الجرائم الإليكترونية من استغلالها ومنها :-

- ضعف المستوى الأمني لواجهات الويبWEB INTERFACES في بيئة الإنترنت.
- افتقار المعايير والمقاييس الموحدة للتواصل بين الأجهزة الطرفية والإنترنت يعوق تعزيز المستوى الأمني في بيئة الإنترنت.

[9] -Manish Gupta and Raj Sharman , Social and Organizational Liabilities in Information Security , publishing Information Science Reference , Hershey , New York , 2009 .P.296

- قلة الرقابة القانونية بين الحكومات في مجال الإنترنت تزيد من فرص القرصنة الإليكترونية.

- أكثر الناس المستهدفين في الاختراقات الأمنية هم الأشخاص الذي يقومون بتصفح الإنترنت حيث يتسبب الاختراق في مشاكل مزعجة مثل بطيء حركة التصفح وانقطاعه على فترات منتظمة ويمكن أن يتعذر الدخول إلى البيانات وفي أسوأ الأحوال يمكن اختراق المعلومات الشخصية للمستخدم.
- في حالة وجود أخطاء برمجة أو إعدادات خاطئة في خادم الويب فمن الجائز أن تسمح بدخول المستخدمين عن بعد غير المصرح لهم إلى الوثائق السرية المحتوية على معلومات شخصية أو الحصول على معلومات حول الجهاز المضيف للخادم مما يسمح بحدوث اختراق للنظام .

- تحدي الحق في الخصوصية يعد الحق في الخصوصية من أسمى الحقوق المدنية الأصيلة للإنسان ،أو حقه في احترام حياته الخاصة فهذا الحق أصبح مهما فالفرد لا يعيش فقط لمصالحه المادية ،وإنما يلزم لحياته حقوق ملتصقة لشخصيته ملازمة لها([١٠]).

والسؤال الذي نحن بصدد ، من صاحب الحق في التمتع بالحق في الخصوصية وبالتالي تشمله الحماية ؟ ، في الإجابة على هذا التساؤل اتجاهان .

الاتجاه الأول :- يقصره فقط على الشخص الطبيعي باعتباره من الحقوق اللصيقة بالشخصية .

---

[١٠] - أحمد فتحي سرور :- الحق في الحياة الخاصة ، مجلة القانون والاقتصاد للبحوث القانونية والاقتصادية ، مطبعة جامعة القاهرة ، العدد٥٤، ١٩٨٦م ، ص ٣٥.، أسامة عبد الله قايد :- الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، بدون دار نشر ورقم طبعة ، ١٩٨٠ ، ص ١٤ ، هشام محمد فريد :- الحماية الجنائية للإنسان في صورته ، مكتبة الآلات الحديثة ، أسيوط ، ص ٧٠.

-Samuel D. Warren &Louis D. Brandeis , The right of piracy , Harvard law review , Vol. IV., Dec. 15, 183-220.

الاتجاه الثاني:- يبسط هذا الحق إلى الأشخاص الاعتبارية للتمتع ضمن نطاق الخصوصية المعلوماتية ([11])

ونحن نؤيد بالطبع الاتجاه الثاني نظرا لتزايد الاعتماد على النظم المعلوماتية ليس فقط على مستوى الشخص الطبيعي ، بل وعلى مستوى الشخص الاعتباري التي تتماثل مع الشخص الطبيعي ، فضلا عن دورها في التنمية والاعتماد الاقتصادي عليها.

ذلك حرصت مختلف الاتفاقيات الدولية المعنية بحقوق الإنسان والحريات والدساتير الوطنية ، ومختلف القوانين الوطنية على وضع العديد من الضوابط الشرعية ، والإجراءات الماسة بالحقوق والحريات الفردية ، ومن ثم فإن مخالفة هذه النصوص في تحصيل الدليل الجنائي يضفي عليه عدم المشروعية ، وعليه فإن الدليل أيا كان نوعه متى تعارضت طريقة الحصول عليه والقواعد القانونية العامة التي توجب احترام حقوق الإنسان وحرياته وقيم العدالة وأخلاقياتها والنزاهة في الحصول على الأدلة واحترام حقوق الدفاع ([12]).

---

[11] – من أنصار الاتجاه الأول الفقيهين فيريه FERRIER، وليندون LINDON ويرى عدم الاعتراف بالحق في الخصوصية للشخص المعنوي استنادا إلى القانون الفرنسي الصادر ١٧ يونيه١٩٧٠، ومن أنصار الاتجاه الثاني الفقيه الفرنسي بيركاير الذي يرى أنه ليس هناك ما يمنع الشخص المعنوي بهذا الحق وسار على هذا النهج الفقه البلجيكي للمزيد راجع :- جلاد سليم :- الحق في الخصوصية بين الضمانات والضوابط في التشريع الجزائري والفقه الإسلامي ، رسالة ماجستير ، كلية العلوم الإنسانية والحضارة الإسلامية ، جامعة وهران ، الجزائر ٢٠١٣-٢٠١٤م ص ٦٦.، آدم عبد البديع آدم حسين :-الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي ، رسالة دكتوراه ،كلية الحقوق ، جامعة القاهرة ،٢٠٠٠م ، ص ٤١٢.

[12]- على سبيل المثال فإن النظام اللاتيني يشترط من أجل أن يستطيع القاضي الاستناد إلى دليل معين ، عليه أن تكون طريقة الحصول على الدليل قد جرت بصورة مشروعة ، وذلك لأن القاضي الجنائي ليس له مطلق الحرية في تكوين عقيدته من الأدلة غير المشروعة التي يتحصل عليها ، ومن الأمثلة لذلك الحصول على الدليل بالإكراه أو التهديد ، أو تفتيش باطل راجع:- ممدوح خليل بحر :- نطاق حماية الحياة الخاصة في القانون الجنائي ، دار الثقافة للنشر والتوزيع ، الأردن ، ٢٠٠٦م ، ص ٣٠٣.
- Todd G. Shipley, Henory R. Reeve, Collecting evidence from a running computer , The national consortium for justice information and statistic ,2006, p.4

وعليه فإن الدليل الجنائي بما فيها الأدلة الرقمية لا يكون مشروعا ومن ثم الاعتماد عليه أمام القضاء الجنائي إلا إذا كان الحصول عليه في إطار أحكام القانون ، وقيم العدالة وأخلاقياتها التي يحرص على حمايتها([١٣]).

ثانيا التهديدات الأمنية للمعلومات الإليكترونية في النظام المعلوماتي :-

يمكن تعريف التهديدات الأمنية بطرق مختلفة تنطوي جميعها على بعض القواسم المشتركة التي تجسد الإطار العام للتهديد بمفهومه الواسع :-

- الشخص ، المنظمة ، الآلية أو الحدث الذي يمكن أن يلحق بالموارد المعلوماتية للمنظمة.
- أي ظرف أو حدث من المحتمل أن يؤثر سلبا على العمليات التنظيمية والأصول التنظيمية والأفراد والمنظمات الأخرى من خلال تعديل المعلومات أو الحرمان من الخدمة ([١٤])

١٣- عائشة بن قارة مصطفي :- حجية الدليل الإليكتروني في مجال الإثبات الجنائي ، دار الجامعة الجديدة الإسكندرية ،٢٠٠٩م ، ص ٢١٣، علي محمود علي حمودة :- الأدلة المتحصلة من الوسائل الإليكترونية في إطار نظرية الإثبات الجنائي ، مقدم للمؤتمر العلمي الأول حول الجوانب القانونية الأمنية للعمليات الإليكترونية ، أكاديمية شرطة دبي ، ٢٨-٢٠٠٣/٤/٢٩م ، ص ٢٠٢ ، ممدوح عبد الحميد عبد المطلب ، زبيدة محمد قاسم ، عبد الله عبد العزيز، أنموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر ، مؤتمر الأعمال المصرفية الإليكترونية ، كلية الشريعة والقانون ، الإمارات ، غرفة تجارة وصناعة دبي، ٥-٢٠٠٣/١٢/١٠م.

- ويرى البعض أن الاستعانة بوسائل علمية حديثة تهدف من استخدامها الحصول على دليل على وقوع الجريمة يستهدف المصلحة العامة ،وذلك حتى تتمكن الدولة من حماية النظام الاجتماعي لا يجوز التذرع باحترام الحقوق والحريات للاعتراض على الدليل بحجه عدم مشروعيته راجع فاطمة مرينز:- الاعتداء على الحق في الحياة الخاصة عبر شبكة الإنترنت ، رسالة دكتوراه ، جامعة أبو بكر بلقان ، تلمسان ، الجزائر ،٢٠١٢-٢٠١٣م .

- بيد أننا لا نتفق مع هذا الرأي حيث أن قاعدة وجوب مشروعية الدليل وطرق الحصول عليها من الرواسخ القانونية والتي لا يجب أن يرد عليها أية استثناءات ، حتى لا نفتح الباب على مصراعيه أمام التعسف في انتهاك الحق في الخصوصية ، الذي أصبح من المبادئ فوق الدستورية، وقد حرص الدستور المصري٢٠١٤ على النص على هذه الحريات الأساسية فقد جاء في المادة٥٧ من النص علي أن حرمة الحياة الخاصة هي مصونة ولا تمس ، والمادة٧٠ حرية الصحافة والنشر .

[١٤] - ممدوح الشحات صقر ، ورقة عمل مقدمة في ندوة حماية نظم المعلومات في المؤسسات العربية ، القاهرة ، ٢٠٠٧م.

- الخطر المحتمل الذي يمكن أن يتعرض له نظام المعلومات قد يكون شخصيا كالمتجسس ، أو المجرم المحترف والقراصنة ، أو شيء يهدد الأجهزة والبرامج والمعطيات ، أو حدث كالحريق أو انقطاع الكهرباء أو الكوارث الطبيعية ([١٥])

ومن خلال ذلك تتحدد أبعاد مفهوم التهديدات الأمنية على النحو التالي :-

- التهديدات توجد متى وجدت نقاط الضعف ، ويمكن أن يوجد أكثر من تهديد لكل نقطة ضعف
- قد تتسبب المشكلات الفنية نتيجة للهجمات المختلفة التي يتعرض لها النظام ، فغالبا تدخل الفيروسات في النظام من خلال البرمجيات المصابة وبعض الوسائل الفنية المستخدمة لتعطيل النظام وتشويهه وعرقلة وظائفه المختلفة ، وإتلاف أو تحريف بياناته ([١٦])

المطلب الثالث

تصنيفات وأساليب التهديدات الأمنية

أولا تصنيفات التهديدات الأمنية

١- نوع الهجوم المحتمل :- حيث يقسم الخبراء المختصين التهديدات الأمنية لأمن المعلومات إلى نوعين (هجوم تقنى وغير تقني)

٢- من حيث المصادر التي تنبع منها التهديدات (داخلية وخارجية)

٣- حسب طبيعة التهديدات (طبيعية – بشرية – بيئية)

٤- – نوع الحدث الحاصل وهو الأساس الذي يحدث لأنظمة المعلومات وهي الكشف والوصول غير المصرح له للمعلومات ،والخداع ، والتحكم غير الشرعي لأجزاء النظام([١٧])

---

١٥ – محمد محمد الألفي ، ورقة عمل مقدمة في ندوة حماية نظم المعلومات في المؤسسات العربية ، القاهرة ، ٢٠٠٧م.

[١٦] – ممدوح الشحات صقر ، مرجع سابق .

[١٧] – هيثم حمود الشبلي ، إدارة مخاطر الاحتيال في قطاع الاتصالات ، دار صفاء للنشر والتوزيع ، ط١ ، عمان ، الأردن ٢٠٠٩ م ، ص٩٤.

وسنركز على أنواع التهديدات من كونها داخلية وخارجية ، وهي تهديدات بشرية تعرف بأنها أي أحداث تتم عن طريق أخطاء البشر سواء أكانت متعمدة أو غير متعمدة

أ. اختراق الشبكات الداخلية للمؤسسات.

ب. اختراق نظم المعلومات بالسرقة أو التبديل أو التغيير أو الحذف.

ت. إيجاد وتهيئة ثغرات في النظام الأمني للشبكات.

ث. تغيير تهيئة نظام شبكات المعلومات.

وقد أظهر تقرير صدر في الولايات المتحدة الأمريكية عام ٢٠٠٣ أن ٣٦% من الجهات تعتبر أن المستخدمين الداخليين هم أشد خطراً على أنظمة المعلومات المتاحة داخل هذه المؤسسات من الخطر الخارجي.

ولكن ولأسباب إعلامية والحفاظ على هيبة الشركات والمؤسسات فإن معظمها تركز سياساتها على عمليات تأمين شبكات المعلومات فيها من الأخطار الخارجية دون الداخلية، وهنا يمكننا طرح تساؤل مشروع حول الدوافع التي يمكن أن تدفع أحد العاملين في مؤسسة أو حكومة ما إلى انتهاك سرية المعلومات المتاحة وشن هجوم يمكن أن يضر بهذه الجهة التي يعمل بها؟ ونجد الإجابة على ذلك في النقاط التالية:-

١-حالات عدم الرضا. فكثيراً ما توضح تحقيقات حالات الاختراق الأمني الداخلي لشبكات المعلومات عن أن السبب كان هو وجود حالة من عدم الرضا عند من قام بالعمل تجاه الجهة التي يعمل بها، سواء كانت هذه الحالة عدم الرضا المادي أو الوظيفي أو الانتقام من مدير أو ما إلى ذلك من أسباب شخصية.

٢-إثبات الذات. أحياناً ما ينتاب العاملون في حقول المعلومات بعض لحظات الأنانية التي يشعر فيها الفرد بحاجته لإثبات قدرته على اختراق الحواجز وانتهاك خصوصية الشبكة، أو الوصول إلى قواعد بيانات محمية بجدران سرية، وما إلى ذلك لمجرد أن يرضي غروره أنه قادر على التحدي، أو الشهرة كما يحدث في حالات كثيرة من اختراق الهاكرز للمواقع الحكومية في

كافة أنحاء العالم، وقد ساعد انتشار برامج كسر الحماية والاختراق الكثير على محاولة تنفيذ هجمات لخرق الشبكات.

٣-الاستفادة المادية. قد يكون الاختراق في حالات مدفوع الأجر من جهات منافسة بغرض الضرر أو إلحاق الهزيمة أو سرقة معلومات أو ما إلى ذلك، فتقوم بعض الشركات والمؤسسات برشوة بعض الأشخاص بغرض تسريب المعلومات واختراق شبكات المعلومات نظير مبالغ مالية.

ثانيا المهاجمون من الخارج وهم أشخاص من خارج النظام المعلومات ويطلق عليهم لقب القراصنة HAKER وهم أكثر خطورة من الفئة الأولي ( ) ، فان فعل الإنسان الذي يشارك من خلال السلوكيات المتعمدة ، ومثالها التخريب والالتقاط المتعمد للبيانات والتعديل غير المبرر، وحذف البيانات ،وسرقة النسخ الاحتياطية والتخريب وتحميل البرمجيات الخبيثة ، والوصول غير المصرح للمعلومات السرية.

أولا : المهاجمون من الداخل أو ولاً: الخطر الداخلي Internal

يقصد بالخطر الداخلي المهاجمون من داخل نطاق عمل شبكة المعلومات، وهم الأفراد أو العاملون الذين ينتمون لنفس الجهة المستهدفة، ولعل هذا النوع من الخطر هو أشد فتكاً وخطورة من خطر الأعداء الخارجيون، ويمثل ذلك التهديد الأكبر للمؤسسات سواء كانت شركات أوهيئات حكومية أو حتى الحكومات نفسها، فخطر انتهاك الخصوصية من الداخل سهل الحدوث وصعب الكشف عنه في حالات كثيرة، وخصوصاً إذا الشخص المهاجم يمتلك صلاحية الولوج إلى نظام شبكات المعلومات فلا يواجه أي صعوبة في عمليات الأمان والسرية الموجودة على الشبكة بل ويمكنه طمس معالم الهجوم ويمحو آثار أي دخول بسهولة، ويمكن إيجاز أهم جوانب الأخطار الداخلية فيما يلي:-

أ. اختراق الشبكات الداخلية للمؤسسات.

ب. اختراق نظم المعلومات بالسرقة أو التبديل أو التغيير أو الحذف.

ت. إيجاد وتهيئة ثغرات في النظام الأمني للشبكات.

ث. تغيير تهيئة نظام شبكات المعلومات.

وقد أظهر تقرير صدر في الولايات المتحدة الأمريكية عام ٢٠٠٣ أن ٣٦% من الجهات تعتبر أن المستخدمين الداخليين هم أشد خطراً على أنظمة المعلومات المتاحة داخل هذه المؤسسات من الخطر الخارجي

ولكن ولأسباب إعلامية والحفاظ على هيبة الشركات والمؤسسات فإن معظمها تركز سياساتها على عمليات تأمين شبكات المعلومات فيها من الأخطار الخارجية دون الداخلية، وهنا يمكننا طرح تساؤل مشروع حول الدوافع التي يمكن أن تدفع أحد العاملين في مؤسسة أو حكومة ما إلى انتهاك سرية المعلومات المتاحة وشن هجوم يمكن أن يضر بهذه الجهة التي يعمل بها؟ ونجد الإجابة على ذلك في النقاط التالية:-

١-حالات عدم الرضا. فكثيراً ما توضح تحقيقات حالات الاختراق الأمني الداخلي لشبكات المعلومات عن أن السبب كان هو وجود حالة من عدم الرضا عند من قام بالعمل تجاه الجهة التي يعمل بها، سواء كانت هذه الحالة عدم الرضا المادي أو الوظيفي أو الانتقام من مدير أو ما إلى ذلك من أسباب شخصية.

٢-إثبات الذات. أحياناً ما ينتاب العاملون في حقول المعلومات بعض لحظات الأنانية التي يشعر فيها الفرد بحاجته لإثبات قدرته على اختراق الحواجز وانتهاك خصوصية الشبكة، أو الوصول إلى قواعد بيانات محمية بجدران سرية، وما إلى ذلك لمجرد أن يرضي غروره أنه قادر على التحدي، أو الشهرة كما يحدث في حالات كثيرة من اختراق الهاكرز للمواقع الحكومية في كافة أنحاء العالم، وقد ساعد انتشار برامج كسر الحماية والاختراق الكثير على محاولة تنفيذ هجمات لخرق الشبكات.

٣-الاستفادة المادية. قد يكون الاختراق في حالات مدفوع الأجر من جهات منافسة بغرض الضرر أو إلحاق الهزيمة أو سرقة معلومات أو ما إلى ذلك، فتقوم بعض الشركات والمؤسسات برشوة بعض الأشخاص بغرض تسريب المعلومات واختراق شبكات المعلومات نظير مبالغ مالية.

ثانيا المهاجمون من الخارج وهم أشخاص من خارج النظام المعلومات ويطلق عليهم لقب القراصنة HAKER وهم أكثر خطورة من الفئة الأولي ، فان فعل الإنسان الذي يشارك من خلال السلوكيات المتعمدة ، ومثالها التخريب والالتقاط المتعمد للبيانات والتعديل غير المبرر،

وحذف البيانات ،وسرقة النسخ الاحتياطية والتخريب وتحميل البرمجيات الخبيثة ، والوصول غير المصرح للمعلومات السرية.

ثانيا المهاجمون من الخارج وهم أشخاص من خارج النظام المعلومات ويطلق عليهم لقب القراصنة HAKER وهم أكثر خطورة من الفئة الأولي ، فان فعل الإنسان الذي يشارك من خلال السلوكيات المتعمدة ، ومثالها التخريب والالتقاط المتعمد للبيانات والتعديل غير المبرر، وحذف البيانات ،وسرقة النسخ الاحتياطية والتخريب وتحميل البرمجيات الخبيثة ، والوصول غير المصرح للمعلومات السرية.-

أساليب التهديدات الأمنية للمعلومات الإليكترونية:-

القرصنة :-

القرصان هو الشخص الذي يتجاوز عناصر التحكم في الوصول إلى النظام من خلال الاستفادة من نقاط الضعف الأمنية التي تركها مطوري الأنظمة في النظام SYSTEM'S VULNERABILITY، بالإضافة إلى براعة المتسللين في اكتشاف كلمات السر ، وتمثل القرصنة تهديدات خطيرة للمعلومات السرية في أنظمة الحاسب([١٨]).

الاختفاء :-**المتخفي أو المقنع** MASQUERADERS هو المستخدم الذي حصل على كلمة المرور لمستخدم أخر على النحو الذي يمكنه من الوصول إلى الملفات المتاحة للمستخدم الآخر

سرقة كلمة السر Password cracking ،اختراق الشبكة والاطلاع عل المعلومات الخاصة بالشركة من خلال سرقة كلمة السر الخاصة بالمعنيين داخل الشركة.

التحميل للملفات دون حماية حيث يتم نقل الملفات من بيئة أمنة في الحاسب المصنف إلى الحاسبات الصغيرة غير المحمية([١٩])

---

[18] - Romney , M& Steinbart ,P. , Accounting information's system ,12ed., ENGLAND. Pearson education,2012.

[١٩] – أشرف صلاح الدين ، طرق الحماية التكنولوجية بأنواعها وأشكالها المختلفة ، ورشة عمل بعنوان أمن وحماية نظم المعلومات في المؤسسات العربية ، القاهرة ، ٢٠٠٧.

– **أحصنة طروادة** TROJAN HORSE . وهو برنامج يظهر بأن يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم مثل الإضرار بالحاسوب أو إرسال معلومات إل المحتال.([٢٠])

–التعرض للاختراق أثناء محاولة معالجة اختراق سابقZERO-DAY-ATTACK

– الهندسة الاجتماعية SOCIAL ENGINEERING ويقصد بها تحفيز المستخدم على الإفصاح عن بيانات سرية من خلال طرح أسئلة بسيطة بهدف جمع معلومات دون إثارة أي شبهة.

– **هجمات حقن قواعد البيانات** مثال من خلال إدخال برمجية ضارة مكان كلمة السر أو اسم المستخدم إذ تمكن المحتال من الوصول إل قواعد البيانات بهدف سرقتها أو التعديل فيها أو تدميرها([٢١]).

شبكات المناطق المحلية حيث تشكل هذه الشبكات تهديدا خاصة للسرية لأن البيانات تتدفق من خلال LAN يمكن مشاهدتها في أي عقدة في الشبكة .

الأجهزة المحمولة والتي تعد من التحديات الجديدة التي تتزايد خطورتها يوما بعد يوم من خلال البرمجيات الضارة التي تستهدفه ، وسرقة البيانات ، وفقدانها وسرقتها ، وقضايا أخرى تظهر في كل وقت مثل القدرة على تحديد الموقع الجغرافي للفرد من خلال أجهزتهم .

---

[٢٠] – ذيب بن عايض القحطاني ، أمن المعلومات ، مدينة الملك عبد العزيز للعلوم التقنية ، الرياض ١٤٣٦هـ – ٢٠١٥م ، ص ٢١٨ وما بعدها .

[٢١] - يوسف خليل يوسف عبد الجابر ، مدى فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإليكترونية في الشركات الصناعية الأردنية ، رسالة ماجستير ، جامعة الشرق الأوسط ،٢٠١٣م ، ص٢٨.

المبحث الثاني

المواجهة التقنية والتشريعية لحماية أمن المعلومات وإشكاليات ذلك

امن المعلومات هو قضية تبحث في نظريات وإستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها. ومن زاوية تقنية، هو الوسائل والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. ومن زاوية قانونية، فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهذا هو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها.

إن أغراض أبحاث وإستراتيجيات ووسائل أمن المعلومات – سواء من الناحية التقنية أو الأدائية – وكذا هدف التدابير التشريعية في هذا الحقل، ضمان توفر العناصر التالية لأي معلومات يراد توفير الحماية الكافية لها:

١- السرية أو الموثوقية : Confidentiaty وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخوّلين بذلك.

٢- التكاملية وسلامة المحتوى : Integrity التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به، وبشكل خاص، لن يتم تدمير المحتوى أو تغييره أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.

٣- استمرارية توفر المعلومات أو الخدمة : Availablity التأكد من استمرار عمل النظام المعلوماتي، واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها.

٤- عدم إنكار التصرف المرتبط بالمعلومات ممن قام به : Non-repudiation ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها، إنكار انه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات أن تصرفا ما قد تم من شخص ما في وقت معين.

وسوف نقوم بتقسيم دراستنا لهذا المبحث وسنتعرض بإيجاز للمواجهة التقنية لأمن المعلومات وفي الشق الثاني المواجهة القانونية لأمن المعلومات وهو ما سنقوم بالتركيز

عليه باعتباره مجالنا التخصصي تاركين التفصيل في الشق الأول للخبراء المختصين وإنما أردنا التعرض إلية لاكتمال التناول للدراسة بشقيها التقني والتشريعي.

المطلب الأول

المواجهة التقنية لحماية أمن المعلومات والمعوقات التطبيقية لذلك

تتمثل أهم الطرق التقنية لحماية أمن المعلومات في الأتي :-

- أن تكون النسخة التي يحصل عليها مقتني البرامج مغلفة بغلاف الشركة المنتجة بشكل محكم ، وهذا لا يعني خلوها تماما من الفيروسات ولكن يقلل من ذلك إلى حد كبير ([٢٢])
- عمل نسخة احتياطية باستخدام القرص الأصلي ، ثم حماية القرص الاحتياطي
- تحميل البرنامج على القرص الصلب من القرص الأصلي للبرنامج.
- مقارنة الملفات المخزنة على القرص الأصلي بنفس الملفات المخزنة على القرص الاحتياطي ، وفي حالة الاختلاف يكون هناك شك بوجود فيروسات.
- العمل على اختبار كل برنامج موجود على القرص للتأكد من أنه يؤدي وظائفه بصورة طبيعية ، وملاحظة أية أشياء غريبة تحدث على البرنامج.
- العمل على اختبار البرامج المخزنة مع تغيير التاريخ في ساعة النظام SYSTEM CLOCK ، وإدخال التواريخ التي تستخدمها بعض الفيروسات التي تبدأ عملها وفق تاريخ أو توقيت محدد ، وبهذه الطريقة يتم كشف الفيروسات والتخلص منها.
- العمل على اختبار البرامج للبحث عن سلاسل طرفية ترتبط بوجود أنواع معينة من الفيروسات وبالتالي إمكانية التخلص منها.
- مراقبة ملفات الأوامر المجمعة BATCH FILES ذات الامتداد BAT من وقت لآخر ، وكذلك ملفات المواصفاتCONFIG. DYSTEM وملاحظة أي تغيير يطرأ على الأوامر الموجودة فيها ، حيث أن أي فيروس يحتاج إلى الارتباط بأية ملفات منفذة حتى يتم تشغيله .
- تعقب آثار الفيروس باستخدام أسلوب التوقيع الرقمي ، حيث يمكن تعقب آثار الفيروسات إلى مصدره عندما يكون الفيروس موجها عبر شبكات الاتصال حيث يتم عن طريق AUDIT TRAIL تتبع هذا الفيروس وتحجيم مروجوه([٢٣])

---

[٢٢] – محمد فهمي طلبة ، فيروسات الحاسب وأمن البيانات ،مجموعة النيل العربية للطباعة والنشر ،١٩٩١م ،ص٩٥.

- إتاحة الإمكانية للبرامج للقيام بعملية الدفاع الذاتي ، حيث يستطيع كل مصمم برامج تصميم نظام دفاعي ضد الفيروسات .
- استخدام أحد البرامج المساعدة في عرض أسماء الملفات المختصة HIDDEN FILES وعند ملاحظة أي أسماء جديدة أكثر من الملفات المستخدمة في نظام التشغيل يكون هناك شك في وجود فيروس يجب التخلص منه.
- تسجيل بيانات كل برنامج مثل حجم الملف والتاريخ والوقت والمصدر وتبدو أهمية هذه البيانات عند ظهور فيروس، حيث يمكن من خلال تاريخ اكتشاف الفيروس استنساخ النسخ الاحتياطية والتي تم عملها قبل هذا التاريخ ويصير الشك في النسخ التالية لهذا التاريخ، وقد تقود إلى تحديد من قام بوضعه.
- وضع برنامج عازل للفيروسات بالجهاز الذي يصل بين الشبكات الداخلية والعالم الخارجي مثل الوسيط PROXY لمنع وصول الفيروسات إلى الشبكة المحلية ، أو إلى أجهزة المستفيدين.
- التأكد من أن جميع الاتصالات التي تتم من خلال الحاسبات الشخصية للمستفيدين بخارج المؤسسة تتم عن طريق الشبكة وليس عن طريق مودم يتم تركيبه خلسة في أحد الحاسبات الشخصية للاتصال بالإنترنت.
- استخدام التوقيع الإليكترونيDIGITAL SIGNATURE فيما يتم تداوله من بيانات داخل الشبكات والبريد الإليكتروني والمصادر الهامة للفيروسات مما يساهم في اكتشافه قبل عمله ، ومن خلال هذا النظام يمكن أن يتحقق نظام التشغيل من صحة التوقيعات على البرامج قبل السماح بتشغيلها ، وبذلك تتضاءل فرص النجاح أمام أي فيروس .

معوقات حماية أمن المعلومات

أن المواجهة التقنية وحدها لا تكفي لحماية أمن المعلومات ، فمما لاشك فيه أن تفعيل السبل القانونية وبناء النصوص الموضوعية في مخاطر التهديدات الأمنية سيؤدي بلا شك إلى تقليص حجم المخاطر وخفض مستوى الجريمة المرتكبة بحق المعلومات عن طريق الاعتداء عليها ، وقد حدثت أغلب الجرائم الإليكترونية الواقعة على النظام المعلوماتي نتيجة علم الجناة بحقيقة النقص والفراغ القانوني الذي يعد عاملا محفزا لهم في المقام الأول على ارتكاب مثل هذه الأفعال لعلمهم بإمكانية إفلاتهم من العقاب.

---

٢٣ - عوض الحاج على أحمد ، عبد الأمير خلف حسين ، أمنية المعلومات وتقنيات التشفير ، دار الحامد للنشر والتوزيع ، الأردن ،٢٠٠٠م ص١٢٨ وما بعدها.

وقد رأينا قبل التعرض للمواجهة التشريعية لأمن المعلومات وحمايته أن نتعرض لأهم المعوقات التي قد تعيق تطبيق القانون ، والتي تحتاج إلى حلول جدية وموضوعية للحيلولة دونها ، وعقب ذلك نتعرض للأطر القانونية والتشريعية لحماية أمن المعلومات سواء على المستوى الدولي أو الوطني وعلى المستوى المحلي لتحقيق أقصى درجات الاستفادة من الدراسة المقارنة.

المعوقات التطبيقية القانونية

تتمثل أهم المعوقات التطبيقية التي تواجهه أمن المعلومات في البيئة الإليكترونية في العراقيل الآتية:-

- ١- في مجال الاعتداء بالفيروسات لا يتمكن الضحية غالبا من معرفة المجرم الذي صمم هذا الفيروس ، وحتى في حالة معرفته فإن الوصل لذلك يحتاج لتكاليف باهظة للوصول لهذه الحقيقة ([٢٤])
- ٢-رغبة العديد من ضحايا الفيروسات وبخاصة الشركات والقطاعات المالية الكبرى ، وبخاصة البنوك في عدم الكشف عن تعرضهم لمثل هذا النوع من الاعتداءات حتى لا تتعرض لهزات اقتصادية قد تعصف بها وتضعف ثقة العملاء بها وسحب الأرصدة الأمر الذي يعرضها للانهيار .
- ٣- جهل أو عدم معرفة الضحية أن نظامه قد أصيب بالفيروس لمدة طويلة ، وعندما يكتشف ذلك يصعب عليه تحديد وقت وسبب الإصابة.
- ٤- صعوبة قياس أو تقدير الخسائر ، وخصوصا عندما تتمثل الخسائر في إتلاف أحد البرامج لإصابة مخططه بالإحباط ، وبخاصة عندما تكون أهمية هذه المخططات تفوق بكثير التقديرات المتوقعة.
- ٥- قدرة الفيروس على إخفاء أي آثار ، وكذا إمكانية بعض الفيروسات مسح نفسها تماما من على ذاكرة البرنامج بعد تنفيذها لغرضها التدميري ، وبالتالي صعوبة الوصول إلى مخططها ، أو من قام بإدخالها إلى النظام.
- ٦- جهل المستخدم للمعلومات الكافية عن الفيروس ، وبالتالي لا يعلم أن هناك مخربا وراء هذا الفيروس ، ويجب الإبلاغ عنه حتى يمكن الوصول إلى مدبره ومعاقبته.
- ٧-عدم توافر الخبرة الكافية لدى المشرعين بالجوانب الفنية المختلفة لموضوع الهجوم الفيروسي ، أو في مجال الحاسب الآلي بصفة عامة ، الأمر الذي يلقي بظلاله على

---

[٢٤] - محمد فهمي طلبة ، مرجع سابق ، ص٢٠٦.

البناء القانوني ، الذي يتطلب معرفة وثيقة بوسائل الاعتداء الفيروسي وتنفيذ مخططه وبالتالي تدخل المشرع لسد القنوات التي يمكن أن تؤدي إلى إفلات المجرم من العقاب، فلابد قبل البحث عن المسائل القانونية المتعلقة بالإنترنت أن ندرك الطبيعة التقنية لهذه الواسطة المعقدة من وسائط تكنولوجيا المعلومات ،فبدون إدراك هذه الطبيعة يتخلف الشرط الموضوعي لتقييم مدى ملائمة القواعد القانونية القائمة ، ومدى الحاجة إلى إيجاد قوانين تنظم مسائل الإنترنت وعصر المعلومات.([٢٥])

- ٨-قدرة الفيروسات على الانتقال واختراق الحدود الجغرافية المتعارف عليها ، وأصبحت آثارها تطول الآلاف بل الملايين من الأجهزة في عدد كبير من البلدان دون استثناء([٢٦]).

استثناء([٢٦]).

ويجب عند وضع تشريع خاص بحماية الأنظمة المعلوماتية من الاعتداءات الواقعة عليه أن يتضمن الآتي:-

أولا :- خلق أجهزة دولية متخصصة هدفها مراقبة شبكات الاتصال ويكون مهمتها الكشف عن الفيروسات التي تروج عبر الشبكة ، وضبط المخالفات في هذا الميدان ومعرفة مصدرها ومن ورائه ، والجهة المروجة له وتقديمها للمحاكمة ،ويشبه عمل هذه الأجهزة عمل اللجان الدولية ، وتمتاز باشتمالها على عناصر فنية متخصصة في ميدان نظم تكنولوجيا المعلومات مما يتيح لها العمل بالشكل الذي يمكنها من حماية المعلومات الإليكترونية من الانتهاكات التي تتم عبر شبكات الاتصال.([٢٧])

---

[٢٥] – نادية أمين محمد علي ، الفيروسات وطرق الوقاية منها كوسيلة لأمن البيانات ، المؤتمر الدولي الأول حول أمن المعلومات ، نحو تكامل رقمي آمن ، ١٨-٢٠ ديسمبر ٢٠٠٥ ، مسقط عمان.

[٢٦] – فعلى سبيل المثال لو أن شخص مقيم في الولايات المتحدة الأمريكية قام بتصميم فيروس اخترق به عبر الشبكة المعلوماتية الإنترنت مجموعة من الأنظمة على الشبكة وتسبب في إتلاف بياناتي طال العديد من البلدان منها مصر مثلا وتسبب في إعطاب الآلاف الأجهزة الحاسوبية مخلفا خسائر يصعب حصرها ، فما هو الإجراء المتبع وبالأخص القانون وأجب التطبيق .

[٢٧] – جميل زكريا محمود ، الفيروسات وطرق الوقاية منها كوسيلة لأمن البيانات ، المؤتمر الدولي الأول حول أمن المعلومات ، نحو تكامل رقمي آمن ،١٨-٢٠ ديسمبر٢٠٠٥م ، مسقط عمان .

– وقد ترتب على البعد الدولي لهذا النوع من الاعتداءات على أمن وسلامه المعلومات باعتبارها من الجرائم العابرة للحدود الأمر الذي يجعل من المستحيل على الدولة وحدها القضاء عليها الأمر الذي يتوجب معه التعاون الدولي الشرطي لمواجهة هذه الأنشطة الإجرامية ، فقد حرص السكرتير العام للمنظمة الدولية للشرطة الجنائية السيدRGMOND KENDAL في مؤتمر جرائم الإنترنت المنعقد في لندن بتاريخ ٢٠٠٠/١٠/٩م على ضرورة التعاون الدولي في مكافحة جرائم تقنية المعلومات ، وأكد على عدم الانتظار لحين عقد معاهدات والاتفاقيات الدولية ، بل يجب البدء الفوري في مكافحة هذه الأنشطة الإجرامية ، كما حرصت العديد من

ثانيا :- إنشاء قانون خاص ومستقل لتفادي الإشكالات الناجمة عن مشاكل الفيروسات المروجة عبر شبكات الاتصال مما يقتضي وجود تشريع خاص بالحماية من مخاطر الاعتداء على المعلومات ، وليس كل صور الاعتداء.

ثالثا:- توضيح الأعمال التي تشكل جرائم نتيجة الأضرار التي يحدثها الاعتداء على النظام المعلوماتي ولتحقيق مبدأ الشرعية يجب التعاون بين رجال القانون لتجريم كافة مظاهر وأشكال الاعتداء التي يلجأ إليها الفيروس في تحقيق الضرر ، دون إغفال الإشارة إلى ضرورة الاستعانة بأصحاب الخبرة الفنية في هذا المجال.

رابعا:- إعداد وتجهيز إجراءات هيكلية تكفل من خلالها المتضررين من الهجمات الفيروسية الحصول على تعويضات مالية إذا ما أحدثت الأضرار لهم خسائر مادية ، ولتحقيق هذا الهدف يجب على المجتمع الدولي إنشاء شركات تأمين عالمية متخصصة ترتبط مباشرة مع الأجهزة الدولية المكلفة بضبط ومتابعة مبرمجي الفيروسات الإليكترونية بهدف تعويض المتضررين من الأضرار التي خلفها الفيروسات .

المنظمات الدولية الأخرى التي لا يقل دورها أهمية عن دور الأنتربول منها منظمة التعاون الاقتصادي والتنمية OECD ومجموعة الثماني الاقتصادية GROUP OF EIGHT حيث قامت في نوفمبر ٢٠٠٠م في طوكيو بإعداد مجموعة أطلق عليها DIGITAL OPPORTUNITY TASK FORCE لتحقيق أمن تكنولوجيا المعلومات ، كما أنشأ المجلس الأوربي في لوكسمبورج ١٩٩٤م شرطة أوربية لتكون همزة وصل بين أجهزة الشرطة المحلية في دول المنظمة لملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال جرائم الاعتداء على المعالجة الآلية ، وفي ٢٠٠٢/٢/٢٨م تم إنشاء الاورجست من قبل مجلس الإتحاد الأوربي كجهاز يساعد في التعاون القضائي والشرطي لمواجهة الجرائم الخطيرة ، حيث يعد دعامة في فعالية التحقيقات والمطاردات المتبعة من قبل السلطات القضائية الوطنية ، وبخاصة الأنشطة المرتبطة بجرائم الاعتداء على نظام المعالجة الآلية ، كما قام مركز التدريب الوطني عن جرائم الإنترنت بإعداد المشروعات والبرامج التي تهدف إلى مكافحة جرائم الاعتداء على نظم المعالجة الآلية ، راجع عمر محمد أبوبكر يونس ، الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية والجوانب الإجرائية ، دار الثقافة العربية للنشر ، ٢٠٠٤م ، عفيفي كامل عفيفي ، جرائم الكمبيوتر ودور الشرطة والقضاء ، رسالة دكتوراه ، كلية الحقوق ، جامعة الإسكندرية ، ١٩٩٩م.

المطلب الثاني

الاتجاهات التشريعية لأمن المعلومات من الاعتداءات الواقعة عليه

تعددت الاتجاهات التشريعية القانونية المتعلقة بالتعامل مع هذه الظاهرة ، وقد اختلف الاتجاه الفقهي في التعامل القانوني والمواجهة التشريعية لهذه الظاهرة وذلك على النحو التالي :-

الاتجاه الأول ويرى أنصاره لإصدار تشريع خاص للتعامل مع هذه الظاهرة ، وانه يمكن للأجهزة القضائية أن تستعمل الأنظمة القانونية القائمة لضبط وتنظيم الأوجه المختلفة لاستخدام الحواسيب ، فكما تعاملت مع التليفون والفاكس يمكنها التعامل مع أجهزة الحواسيب ([٢٨])، أو الاكتفاء بالحماية الأمنية ذات الطبيعة التقنية.

الاتجاه الثاني ينادي أنصاره بضرورة إصدار تشريع خاص ومستقل عن قانون عن قانون العقوبات للتنظيم التشريعي يتعلق بكل ما يخص النظام المعلومات ([٢٩])

وباستعراض عام للأساليب والأشكال التي تلجأ إليها الدول في صياغة النصوص القانونية بهدف الحماية الجنائية للأنظمة المعلوماتية ، وذلك على النحو التالي :-

- تتجه بعض الدول عند صياغتها للنصوص الجنائية التي تحمي النظام المعلوماتي إلى إتباع أسلوب ومنهج الإضافة بإضافة نصوص تنظيم الحالات التي يرتكب فيها الجاني النشاط الإجرامي المتصل بالنظم المعلوماتية إلى النصوص القائمة والموجودة بالفعل([٣٠])
- فيما تقوم دول أخرى بوضع نصوص علي نصوص تقليدية قائمة بالفعل بصياغة نص جديد يتفق مع أحد الأشكال التقليدية للسلوك الإجرامي ، حيث يتم تحويل السلوك في

---

[٢٨] – إيهاب ماهر السمباطي :-الجرائم الإليكترونية والجرائم السيبرية وظيفة جديدة ، فئة مختلفة ، التناغم القانوني هو السبيل الوحيد ، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر ، المغرب ١٩-٢٠ يونيه ،٢٠٠٧م ، ص٣.

[٢٩] – المرجع السابق ، ص ١٦.

٣٠ – نائل عبد الرحمان صالح ،واقع جرائم الحاسب في التشريع الأردني ، بحيث مقدم لمؤتمر القانون والكمبيوتر والانترنت الذي نظمته كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة) 2000 (بحوث مؤتمر القانون والكمبيوتر والإنترنت ، المجلد الأول ، الطبعة الثالثة ، كلية الشريعة والقانون جامعة(الإمارات العربية المتحدة ، ٢٠٠٤م

صورته التقليدية إلى صورة أخرى ترتبط بالحاسب الآلي ونظامه باعتبارها المحل الجديد للسلوك الإجرامي ، وغالبا ما تتبع أغلب الدول هذه الطريقة.

- وتتجه بعض التشريعات إلى إفراد قانون يعاقب على الجرائم المعلوماتية بكل صورها ، ويكون ذلك إما بإصدار تشريع مستقل ، أو تجميع كل ما يتعلق بالجرائم المعلوماتية في قسم مستقل ملحق بالتشريع الجنائي وضبط الطريقة التي تسمح بتوجيه الطبيعة الخاصة بالجريمة المعلوماتية ، ووضع عقوبات خاصة لهذه الجرائم بما يتوافق معها ومن هذه الدول الولايات المتحدة الأمريكية([٣١]) .
- كما أن بعض الأنظمة القانونية في سبيل الحماية الجنائية للمعلومات قامت بالجمع بين أكثر من أسلوب من أساليب الصياغة التشريعية المتقدمة ، ويرجع سبب ذلك إلى مدى تأثير هذه الجرائم ووقت تدخل المشرع لمواجهتها ، وتعد السويد من الدول التي واجهت بداية الجريمة المعلوماتية بوضع نص عام يتعلق بالجريمة المعلوماتية ن وبعد ذلك قامت بتعديل قانون العقوبات بإضافة نصوص جديدة تنظم الجريمة المعلوماتية قياسا على نصوص قائمة بالفعل في القانون مع الاحتفاظ بالنص الأول المتعلق بالجريمة ذاتها.([٣٢])

---

[٣١] – أشرف شمس الدين ، الحماية الجنائية للمستند الإليكتروني ، ط١ ، دار النهضة العربية ، القاهرة ، ٢٠٠٦م ، ص٩.

[٣٢] نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، رسالة دكتوراه، جامعة القاهرة، كلية الحقوق، طبعة ٢٠٠٣ ،ص.٣١٤-٣١٥.

قانون الأونيسترال النموذجي للتجارة الإليكترونية :-UNCITRAL ([٣٣])

وضعت اللجنة الأممية للقانون التجاري وعرف اختصارا بالاونيسترال في اعتبارها أن هذا القانون يكون أداة فعالة للدول المعنية بتحديث تشريعاتها في إطار التعاملات المتعلقة بتقنية الاتصالات الحديثة ، ولقد طرأ على هذا القانون عدة عمليات تشريعية تكميلية وفق المستجدات الواقعة ، بغية أن يكون قانونا متكاملا .

إن منهج قانون الأونسيترال النموذجي أساسا يقوم علي التسليم بأن الاشتراطات القانونية التي تفرض استخدام "المستندات الورقية التقليدية" و أيضا توفير التوقيع اليدوي الممهور بخط اليد و تقديم أصل المستند لإثباته ... كل هذه الاشتراطات تقف عائقا رئيسيا يحول دون استحداث وسائل "المراسلات" و مستخرجات "الداتا" العصرية المستخدمة في التجارة الالكترونية . أو حتي لو تم استحداثها فهل هي تتمتع بالقوة القانونية اللازمة ؟ و لذا لا بد من النظر في إمكانية المعالجة القانونية للعوائق التي تحول دون استخدام وسائل التجارة الإلكترونية، علي أن يتم ذلك عبر توسيع نطاق المفاهيم الحديثة للتعامل مع "كتابة المستندات" و"أصل المستندات" و "التوقيعات الممهورة علي هذه المستندات" مع ضرورة العمل علي إزالة الفوارق القانونية بين هذه الإشكاليات حتى يتم فتح المجال لتطوير التجارة الالكترونية وفق أسس قانونية سليمة ومتطورة ولسد الفجوة التشريعية التي تحول دون ذلك.

قانون الأونسيترال النموذجي ، و لتحقيق الغرض المنشود ، قام بانتهاج نهجا جديدا يشار إليه بمنهج "النظير الوظيفي" أو "النظير المتكافئ". أي جعل "الداتا" المستند الالكتروني في وضع قانوني مناظر وظيفيا أو متكافئ للمستند الورقي التقليدي. و من أجل هذا كان لا بد من حصر ومعرفة حقيقة الوظيفة التي يؤديها المستند الورقي "التقليدي" و لقد تبين من ذلك أن المستند الورقي "التقليدي" مقروء للجميع ، و أن هذا المستند يبقي دون تحوير بمرور الزمن ، وأن المجال متاح لجميع الأطراف لاستنساخ المستند و الحصول علي نسخة من البيانات نفسها ،

---

[٣٣] – قانون الأونيسترال النموذجي للتوثيق التجاري الدولي مع دليل الاشتراع استعماله ، منشورات الأمم المتحدة ، ٢٠٠٤ .A05.V4.

و أن المجال متاح لتوثيق البيانات بواسطة توقيع من أنشأ المستند ، و أن المجال متاح لوضع المستند في شكل قانوني مقبول لدي السلطات العامة و أيضا المحاكم.

هذه هي الوظائف و المهام التي ظل يقوم بها المستند الورقي التقليدي. ولتطبيق نظرية "النظير الوظيفي" أو "النظير المتكافئ" فيجب إعداد السجلات الالكترونية لتحقيق نفس وظائف المستند الورقي التقليدي مع ضرورة توفير نفس المستوي من الأمان الذي توفره المستندات الورقية. و لمنح المستند الالكتروني القوة الوظيفية النظيرة أو القوة المتكافئة للمستند الورقي فلا بد من استيفاء بعض الاشتراطات التقنية والقانونية كتحديد مصدر البيانات و محتواها مثلا.

و نفس الوضع يتعلق بالتوقيع علي المستند الورقي لإثباته و مع تسليم أصل المستند عند الطلب ليتم اعتماده ، خاصة و أن المستندات الالكترونية بدون توقيع يدوي و عندما تستخرج من الجهاز تكون في شكل صورة وليس أصل. فمثلا عندما تذهب لجهاز الصرف الآلي و تطلب كشف حساب فان الكشف الصادر من الجهاز الآلي سليم لكنه يخلو من التوقيع اليدوي المعتمد و كذلك فان هذا الكشف صدر في صورة مستند آلي و لا يعتبر أصل "أوريجنال"، و بالتالي إذا تم تطبيق اشتراطات القانون العادية فان كشف الحساب هذا يعتبر عديم القوة القانونية لأنه يخلو من التوقيع المعتمد وأيضا فانه صورة "كوبي" و ليس أصل "أوريجنال" و لذا فانه غير مقبول أو غير ملزم.

و لسد هذه الفجوة القانونية فان قانون الاونسيترال النموذجي للتجارة الالكترونية قام باستحداث منهج "النظير الوظيفي أو النظير المتكافئ" بحيث يعتبر المستند الالكتروني "الداتا" كنظير وظيفي أو مكافئ للمستند الورقي التقليدي و يقوم بنفس الوظيفة. و هذا أيضا ينطبق بحيث يعتبر التوقيع الالكتروني "DIGITAL SIGNATURE" أو التوقيع الالكتروني الإجرائي يتمتع بالنظير الوظيفي أو المتكافئ للتوقيع اليدوي الممهور بخط اليد ، وبحيث يكون المستند الالكتروني الصادر من الجهاز الالكتروني كنظير وظيفي و نظير متكافئ للمستند الورقي الأصلي ... و كل هذا بالطبع بعد توفر الاشتراطات القانونية المعينة التي يتضمنها القانون النموذجي.

وبهذا فان المستند الالكتروني المستخدم في التجارة الالكترونية و الصيرفة الالكترونية يعامل ، و وفق القانون ، بنفس الدرجة التي يعامل بها المستند الورقي التقليدي لأن القانون النموذجي منح قوة النظير الوظيفي و النظير المتكافئ للمستند الالكتروني ليقوم بنفس وظيفة المستند الورقي التقليدي تماما و بالتمام و الكمال.

و باستحداث هذا الوضع القانوني بموجب القانون النموذجي قامت كل الدول بإصدار تشريعاتها الوطنية التي بموجبها تم منح القوة القانونية للمستندات الالكترونية التي تتم التجارة و الصيرفة الالكترونية عبرها. وهذا الوضع منح القوة الدافعة للصيرفة الإلكترونية التي فتحت العمل المصرفي لآفاق بعيدة استفاد منها الاقتصاد و التجارة و كل المجتمع. ومن هذا الفتح القانوني الهام تم توفير البيئة القانونية السليمة التي توفر الجو الملائم لنمو و حياة التجارة الالكترونية بكافة أشكالها بين كل أطراف العالم و أركانه المختلفة.. و هكذا القانون يتطور للملائمة مع عصر التكنولوجيا بل ليقود بعث الحياة فيها لفائدة الجميع ...([٣٤])

<u>الاتفاقية الدولية الخاصة بالإجرام المعلوماتي المبرمة ببودابست ٢٠٠١م</u>

وقع على هذه الاتفاقية الدولية الأولى ٣٠ دولة في العاصمة المجرية بودابست ٣٠ دولة وتشمل هذه المعاهدة عدة جوانب من جرائم الإنترنت منها الإرهاب وتزوير بطاقات الائتمان ودعارة الأطفال ، وتقدم هذه الاتفاقية إطار عام وتعتبر الصك الدولي الوحيد الملزم ويوفر إطار عام لتطوير التشريع الوطني الشامل لمكافحة إجرام الإنترنت، ومن أجل جعل هذه الاتفاقية أكثر فعالية فإنها تحتاج إلى توسيع نطاقها وتطبيقها على أوروبا.

بيد أن هذه الاتفاقية لا تتناول سوي الجرائم المرتكبة عن طريق الإنترنت وشبكات الحاسب الأخرى والتعامل بشكل خاص مع التعدي على حق المؤلف المرتبط بالحاسب الآلي والتصوير الإباحي للأطفال وانتهاكات أمن الشبكات.

التشريعات الوطنية لمواجهة الاعتداء على أمن المعلومات

---

[٣٤] – للمزيد راجع وائل بندق ، موسوعة القانون الإليكتروني وتكنولوجيا الاتصال والمعلومات ، دار المطبوعات الجامعية ، الإسكندرية ، ط١ ، ٢٠٠٧م

أولا :- النظام القانوني الأمريكي لمكافحة جرائم المعلوماتية :-

يقوم النظام الأمريكي على مجموعة من التشريعات على المستوى الفيدرالي ، وعلى المستوى المحلي في مختلف الولايات، وسنستعرض ذلك على النحو التالي:-

- **على المستوى الفيدرالي :-**

يمثل الفصل١٨٠ من قانون الولايات المتحدة التشريع الرئيسي لجرائم التقنية الحديثة من خلال سن العديد من القوانين الفيدرالية كان أولها قانون الاحتيال وإساءة استخدام الكمبيوتر أو COMPUTER FRAUD AND ABUSE (CFAA) عام ١٩٨٤م وتم تعديله عام ١٩٨٤م و١٩٩٤م للتعامل مع البرامج الخبيثة لإتلاف أو تغيير البيانات ، ونص القسم ١٠٣٠ من الفصل١٨ على تجريم العديد من الأفعال أهمها :-

- الدخول غير المصرح به إلى أحد أنظمة الحاسب للحصول على معلومات أمنية وطنية بنية الإضرار بالبلاد ،أو لمنفعة دولة أجنبية.
- الدخول غير المصرح به لأنظمة الحاسب الآلي للحصول على معلومات خاصة بأموال محمية.
- الدخول غير المصرح به إلى النظام الخاص بالحكومة الفيدرالية.
- الدخول غير المصرح به إلى أي نظام بنية الاحتيال.
- الدخول غير المصرح به إلى أي نظام مع تعمد إلحاق أضرار به
- الاتجار الاحتيالي في كلمات سر الحاسوبية ، وغيرها من المعلومات للوصول لنظام محمي.
- بث أو تهديد بارتكاب ضرر لأي نظام محمي عبر الولايات المتحدة ، أو للتجارة الأجنبية بغرض ابتزاز أموال ، أو منافع من أي شخص طبيعي أو معنوي.

القسم١٤٦٢ من الفصل١٨ تعلق باستخدام الحاسب لاستيراد مواد مخلة بالآداب ، القسم ٢٢٥١ جرم توظيف أي قاصر أو إغرائه للمشاركة في أنظمة جنسية ، القسم ١٠٢٨ جرم إنتاج ، أو نقل ،أو إدارة تتضمن نظام حاسوبي بقصد استخدامه في تزوير الوثائق ،أو إنشاء وثائق مزورة.

وفي عام ٢٠٠٣م أصدر الكونجرس الأمريكي قانون مكافحة البريد الإليكتروني غير المرغوب فيه(ANTI SPAM LAW) ، ودون في القسم ١٥٣٧ من الفصل١٨ ، ويحظر إرسال الرسائل غير المرغوب فيها ، وأن تشمل رسائل البريد الإليكتروني آلية تتيح للمتلقي الإشارة أنه لا يريد استقبال هذه الرسائل .

وعلى مستوى الولايات المتحدة تملك كل ولاية حرية التشريع الخاص بها والإطار العام لتوحيد قوانين جرائم التقنية يعتمد على مشروع قانون نموذجي MODEL STATE COMPUTER CRIMES CODE الذي تم وضعه من قبل هيئة أكاديمية ١٩٩٨م.([٣٥])

النظام الفرنسي :-

تعتبر فرنسا من أوائل الدول التي تعاملت مع جرائم تقنية المعلومات فقد صدر قانون العقوبات الفرنسي في عام ١٩٩٨ وبموجبه تم تجريم الدخول إلى نظام المعالجة الآلية للمعلومات أو البقاء فيها بطريق غير مشروع وعاقب على ذلك بالحبس مدة تتراوح بين شهرين وعام وبغرامة من٣٠٠٠-٥٠٠٠ فرنك أو بإحدى هاتين العقوبتين،وبعدها صدر قانون رقم ١١٧٠ لسنة ١٩٩٠ والذي اشتملت مادته (٢٨لبيان معنى التشفير وضمان سرية المعلومات والاستيلاء على المعلومات بطريق اختراق التشفير)([٣٦]).

بعدها صدر المرسوم رقم ٩٢-١٣٥٨ في كانون الأول لسنة ١٩٩٢ والمتعلق بالبلاغات والالتماسات للحصول على إذن الترميز المتعلق بالوسائل والتسهيلات ، حيث يبت مواد هذا المرسوم تفاصيل تقديم وتصدير واستخدام خدمات أي نوع من أنواع المرافق المشفرة ،، وبموجبه أيضاً لا تعتبر وسيلة من وسائل الترميز إذا كانت الوسيلة تتعلق بأجهزة ،أو برمجيات خاصة لحماية البرامج من النسخ غير المشروع استخدامها والتي تستفيد من وسائل أو أجهزة سرية شريطة أن لا يسمح التقييد بشكل مباشر أو غير مباشر من خلال البرنامج المعني ، وأخيراً

---

[٣٥] .يونس عرب ، جرائم الكومبيوتر والانترنت ، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات ، ورقة عمل مقدمة إلى مؤتمر الأمن العربي ٢٠٠٢م تنظيم المركز العربي للدراسات والبحوث الجنائية ، أبو ظبي ، ص١١ ، ١٠/ -١٢/٢ ٢٠م.

٣٦ - عبد الفتاح بيومي حجازي،التجارة الإليكترونية وحمايتها القانونية ، دار الفكر الجامعي ، الإسكندرية ،٢٠٠٤م ، ص ص ٣٩-٤١.

صدر قانون العقوبات الفرنسي الجديد لعام ١٩٩٤ والذي عالج بدوره تنظيم المعالجة الآلية للبيانات في المادة ٣٢٣ بفقراتها الأربعة فالفقرة الأولى ذهبت لتجريم الوصول أو البقاء بطريقة مخادعة في كل جزء من نظام المعالجة الآلية للمعطيات ،أما الفقرة الثانية فقد جرمت إعاقة النظام وتزوير المعطيات والمعالجة الآلية ،وما يسجل بشأن القانون الفرنسي الجديد (قانون العقوبات) انه جاء خالياً من الإشارة للجرائم المالية والجرائم التي تهدد الشخصية الفردية والجرائم غير الأخلاقية كما انه جاء خالياً من تجريم المقامرة عبر الإنترنت والاتجار بالبشر وجرائم الاختراقات وصناعة ونشر الفيروسات([٣٧]).

ثانيا التشريعات العربية الخاصة بجرائم أمن المعلومات:-

١- <u>التشريع السعودي ([٣٨])</u>

احتلت المملكة العربية السعودية المركز السادس عالمياً بين الدول التي تنطلق منها الهجمات الالكترونية نسبة إلى عدد مستخدمي الانترنيت في البلاد() ،].فكان لا بد لها من إصدار تشريع خاص بذلك ، حيث سبقت السعودية قانون جديد لمكافحة جرائم المعلوماتية ، فقد صدر المرسوم الملكي رقم م /١٧ في /٨/٣ ١٤٢٨هـ بناء على قرار مجلس الوزراء رقم ٧٩ بتاريخ /٧/٣ ١٤٢٨هـ ، وقد تضمن هذا المرسوم بيان معاني المصطلحات والمسميات ومنها الجريمة المعلوماتية أما المادة الثالثة فقد عاقبت على العديد من الأفعال الجرمية بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة إلف ريال أو بإحدى هاتين العقوبتين وهي التصنت على ما هو مرسل عبر شبكة المعلوماتية ، أو أجهزة الحاسب دون مسوغ نظامي صحيح ، والدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عن القيام به ، والمساس بالحياة الخاصة باستخدام الهاتف النقال المزود بكاميرا وما في حكمها والتشهير بآخرين وإلحاق الضرر بهم عبر وسائل تقنية المعلومات كما أن المادة الخامسة من

---

[٣٧] – محمد حماد مرهج الهيتي، "جرائم الحاسوب" ، ١ط ، إدارة المناهج للنشر والتوزيع ، عمان، ٢٠٠٦م ص١٧٩ ، مفتاح بوبكر المطردي ، الجريمة الإليكترونية ، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية ، السودان٢٣-٢٥ أيلول ٢٠٠١م،مدحت رمضان ، جرائم الاعتداء على الأشخاص والإنترنت ، دار النهضة العربية ، القاهرة ، ٢٠٠٧م ، ص١٧.

٣٨ – نظام مكافحة جرائم المعلوماتية ، هيئة الاتصالات وتقنية المعلومات ، المملكة العربية السعودية .

هذا المرسوم عاقبت بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين الف ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أياً من الجرائم المعلوماتية كالدخول غير المشروع لإلغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها أو إتلافها أو تغييرها أو تدميرها أو مسح البرامج أو البيانات المستخدمة وكذلك إعاقة الوصول إلى الخدمة أو تشويشها أو تعطيلها بأي وسيلة كانت وقد عاقبت المادة السادسة بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب جريمة إنتاج ما من شأنه المساس بالنظام العام أو القيم الدينية أو الآداب العامة أو حرمة الحياة الخاصة أو إعداده أو إرساله أو تخزينه عن طريق شبكة المعلوماتية كما جرمت إنشاء المواقع الخاصة بنشر ما يتعلق بالاتجار بالجنس البشري وتسهيل التعامل به وجرمت أيضا إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها وكذلك ما يتعلق بالمخدرات والمؤثرات العقلية كما جرم هذا المرسوم في مادته السابعة إنشاء المواقع لمنظمات إرهابية على الشبكة المعلوماتية والتعامل معها ومساعدتها والترويج لأفكارها وكل ما يتعلق بنشاطاتها .وقد بين هذا المرسوم الظروف المشددة في هذه الجرائم م ٨ / ووسائل المساهمة الجنائية م ٩ /والعقاب على الشروع في الجرائم التي طواها م /١٠ والحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب هذه الجرائم م /١٣ . وجدير بالذكر إن القانون السعودي كان قد انفرد بالنص على تجريم إنتاج ونشر كل ما من شأنه المساس بالقيم الدينية والاعتداء على الأديان باستخدام وسائل تقنية المعلومات وكذلك تجريمه لإنشاء مواقع للمنظمات الإرهابية ولكل ما يتعلق بها من تمويل ونشر وترويج وغيرها.

موقف التشريع المصري من جرائم الاعتداء على أمن المعلومات :-

وفيما يتعلق بقانون العقوبات المصري فقد وردت المواد ٣٠٩ مكرر (أ) و٣١٠ في شأن حماية الحياة الخاصة ، أما نص المادة ٣١٠ من قانون العقوبات فإنه يجرم إفشاء السر الذي وصل إلى علم 1أصحاب المهن أو الحرف رغم إنهم مؤتمنون على هذه الأسرار([٣٩])

[٣٩] – عبد الفتاح بيومي حجازي ، مرجع سابق ،٦٦٤-٦٦٥.

ومؤخرا أصدر المشرع المصري وحسنا فعل القانون رقم ١٧٥ لسنة٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات([٤٠])

جاءت المادة الأولى منه لتعريف المصلحات الواردة بالقانون ، ونصت المادة الثانية على التزامات وواجبات مقدم الخدمة ومنها الالتزام بالحافظة على سرية المعلومات التي تم حفظها وتخزينها(م٢/٢) ، وكذا التأكيد على تأمين البيانات والمعلومات بما يحافظ على سريتها وعدم اختراقها(م٢/٣) .

ونصت المادة الثالثة على نطاق تطبيق القانون المكاني ، وحرص كذلك القانون على النص على التعاون الدولي في مجال مكافحة جرائم تقنية المعلومات من خلال التعاون الدولي والاتفاقيات الدولية وحرص القانون على أن يكون المركز الوطني لطوارئ الحاسب والشبكات هو المنوط به في هذا الشأن.

وجاء في الباب الثاني من القانون النص على الأحكام والقواعد الإجرائية ومأمورو الضبط القضائي (المواد ٥، ٦) ، وإجراءات حجب المواقع (م٧) ، والتظلم من تلك القرارات (م٨) ، وحرص القانون على التأكيد على حجية الأدلة الرقمية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة في اللائحة التنفيذية بهذا القانون.

وخصص الباب الثالث من هذا القانون للنص على الجرائم والعقوبات فجرم القانون الاعتداء على سلامة شبكات وأنظمة تقنيات المعلومات وجريمة الانتفاع بدون وجه حق بخدمة الاتصالات والمعلومات وتقنيتها (الحبس لمدة ثلاثة شهور وبغرامة لا تقل عن عشرة الآف جنيه ولا تزيد عن خمسين الف ،أو بإحدى هاتين العقوبتين)

كما جرم القانون الدخول غير المشروع سواء بخطأ عمدي أو غير عمدي الدخول غير المشروع به على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه (م١٤) ، وعاقب عليه بالحبس لمدة لا تقل عن سنة وبغرامة لا تقل عن ٥٠٠٠٠ ولا تزيد عن ١٠٠٠٠٠ الف جنية أو بإحدى هاتين العقوبتين.

---

[٤٠] – القانون رقم ١٧٥ لسنة٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات المنشور بالجريدة الرسمية العدد٣٢ مكرر في١٥ أغسطس ٢٠١٨.

كما جرم القانون تجاوز حدود الحق في الدخول (م١٥) ،وكذا الاعتراض غير المشروع بدون وجه حق أي معلومات أو بيانات أو كل ما هو متداول على شبكة المعلومات أو أحد أجهزة الحاسب الآلي أو ما في حكمها(م١٦) ، كما جرم القانون الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية (م١٧) ، وكذا جريمة الاعتداء على البريد الإليكتروني أو المواقع أو الحسابات الخاصة (م١٨) ، وجريمة الاعتداء على تصميم موقع(م١٩).

كما حرص القانون على تجريم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة أو أحد الأشخاص الاعتبارية بالحبس لمدة لا تقل عن عامين وبغرامة لا تقل عن ٥٠٠٠٠ولا تزيد عن ٢٠٠٠٠٠ الف جنيه ، وشدد العقوبة للسجن وغرامة لا تقل عن ١٠٠٠٠٠ ولا تزيد عن ٥٠٠٠٠٠ متى كان الدخول بقصد الاعتراض أو الحصول على بيانات أو معلومات حكومية ، وإذا ما ترتب على ذلك إتلاف أو تدمير لتلك المعلومات أو البيانات تكون العقوبة السجن والغرامة لا تقل عن مليون ولا تجاوز خمسة ملايين جنيه مصري(م٢٠)

كما جرم القانون الاعتداء على سلامة الشبكة المعلوماتية (م٢١) ، وحرص القانون على تجريم حيازة أو إحراز أو جلب أو بيع أو إتاحة أو إنتاج أو صنع أو استيراد أو تصدير كل ما يسهل ارتكاب أيا من الجرائم المنصوص عليها في القانون (م٢٢).

وخصص الفصل الثاني من هذا الباب على الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات والاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإليكتروني (م٢٣) ، والجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإليكتروني (م٢٤).

وخصص الفصل الثالث لجرائم الاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع (م٢٥) ، كما جرم القانون كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى مناف للآداب العامة ، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه (م٢٦).

وخصص الفصل الرابع للنص على الجرائم المرتكبة من مدير الموقع(المواد ٢٧-٢٩) ، ونص الفصل الرابع من القانون على المسئولية الجنائية لمقدمي الخدمة (المواد

٣٠-٣٣)، ونص الفصل السادس على الظروف المشددة في الجريمة وجعل الإخلال بالنظام العام أو تعريض سلامة المجتمع وآمنة للخطر أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو منع أو عرقلة السلطات العامة من ممارسة لأعمالها أو تعطيل أحكام الدستور والقوانين أو الإضرار بالوحدة الوطنية أو السلام الاجتماعي ظروف مشددة تصل بالعقوبة للسجن المشدد(م٣٤).

ونص الفصل السابع على المسئولية الجنائية للشخص الاعتباري(المواد ٣٥-٣٧) ، وجاء الفص الثامن للنص على العقوبات التبعية بمصادرة الأدوات والمعدات والأجهزة المستخدمة(م٣٨-٣٩) ، ونص الفصل الثامن على الشروع والإعفاء من العقوبة (م ٤٠-٤١) ، والصلح والتصالح (م٤٢). ونص الباب. الرابع على الأحكام الانتقالية والختامية(المواد ٤٣-٤٥) .

وقد ألزم القانون مقدمي الخدمة والمخاطبين بأحكامه اتخاذ الإجراءات اللازمة لتقنين أوضاعهم خلال سنة من تاريخ العمل بأحكامه(م٤٣)

المطلب الرابع

مدى ملائمة المواجهة التشريعية والإجرائية لمواجهة الاعتداءات على أمن المعلومات

ثالثا :- مبدأ الشرعية :-

يقصد بالركن الشرعي للجريمة وجود نص تشريعي يوضح العقوبة المترتبة عليه وقت وقوع الفعل ([٤١]) ، فمبدأ الشرعية يمنع المسائلة الجنائية ما لم يتوافر نص تشريعي " لا جريمة ولا عقوبة إلا بنص" ، فمتى انتفى النص التشريعي انتفت الجريمة وامتنعت المسئولية ، وتحقق القصور في مكافحة هذه الجرائم([٤٢])تمثل المشروعية حجر الزاوية للنظام الجنائي بأسره، فمنه تتفرع وحوله تدور كافة المبادئ التي تحكم القواعد الجنائية موضوعية كانت أو إجرائية([٤٣]).

والسؤال محل البحث في هذا الشق هل النصوص القانونية القائمة كفيلة لمعالجة هذه الظاهرة التي من بينها الاستخدام غير المشروع لشبكة الإنترنت؟([٤٤]) ، وتبين من الواقع أنه في بعض الأحوال توجد ثمة أفعال جديدة ترتبط باستعمال الكمبيوتر لا تكفي النصوص الحالية القائمة لمكافحتها منها الاعتداء على حرمة الحياة الخاصة حيث أن تجميع معلومات عن الأفراد وتسجيلها في الكمبيوتر لا تخضع للتجريم وفقا للقواعد العامة ، كما أن التداخل في نظام الحاسب الآلي وتغيير البيانات صورة جديدة لا يعرفها

---

[٤١] – عبد المحسن بدوي محمد أحمد :- إستراتيجيات ونظريات معالجة قضايا الجريمة والانحراف في وسائل الإعلام الجماهيرية ، الندوة العلمية حول الإعلام والأمن ، مركز الدراسات والبحوث ، قسم الندوات واللقاءات العلمية ، أكاديمية نايف العربية للعلوم الأمنية ،١١-١٣ /٥ /٢٠٠٥ ، ص٥

[٤٢] – يونس عرب :- قراءة في الاتجاهات التشريعية للجرائم الإليكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان ، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإليكترونية ، مسقط ، ٢-٤ أبريل ٢٠٠١م، ص٤٣.

٤٣ عبد العظيم مرسي وزير: شرح قانون العقوبات ، دار النهضة العربية ، ص ٣٣.

٤٤ – عبد الجبار الحنيص :- الاستخدام غير المشروع لنظام الحاسوب من وجهة نظر القانون الجزائي " دراسة مقارنة" ، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية ، المجلد٢٧ ، العدد الأول ، ٢٠١١م ، ص ١٩١.

قانون العقوبات قبل ظهور الحاسب الآلي وشبكة الإنترنت ، مما يؤكد وجود قصور القواعد التقليدية في القانون الجنائي على مكافحة هذا النوع المستحدث من الجرائم([٤٥])

من هنا تبدو الحاجة الماسة إلى تدخل المشرع لمواجهة جرائم الإنترنت باعتبارها من المستحدثات التي عجزت مواد القوانين العقابية التقليدية في مواجهتها ، لذلك سعت دول العالم المتقدمة إلى سن التشريعات لمواجهة هذه الظاهرة([٤٦]).

ويتبقي التساؤل هل التوسع في تفسير النصوص القائمة لتطبيقها على جرائم الإنترنت يبقى هو الحل لتلافي هذه الفجوة؟

---

٤٥ – غنام محمد غنام :– عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر ، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت ، الإمارات العربية المتحدة ، كلية الشريعة والقانون ، ١–٣مايو ٢٠٠٣م ، المجلد الثاني ، ص ص ٦٢٥–٦٢٦.

[٤٦] – في فرنسا صدر القانون رقم ١٩ لسنة ١٩٨٨م تحت عنوان " الجرائم في المواد المعلوماتية" ، وادمج في الفصل الثاني من قانون العقوبات وخصصت له المواد من ٤٣٢–٢٨٢–٩/٤٦٢ ، تم تعديله في عام١٩٩٢م ، وفي عام٢٠٠٠م صدر القانون رقم ٢٣٠ بشأن الإثبات المتعلق بالتوقيع الإليكتروني ، وفى الولايات المتحدة الأمريكية وضع قانون خاص بحماية الحاسوب والشبكات ١٩٧٦م ، وعرفت دول أخرى هذا النوع من القوانين مثل ألمانيا عام ١٩٨٦م ، النمسا والنرويج واليابان عام ١٩٨٧م ، واليونان ١٩٨٨م ،وسويسرا١٩٩٤م ،واسبانيا والدانمرك وكندا وفنلندا ١٩٩٥م راجع :– مفتاح بو بكر المطردي :– الجريمة الإليكترونية ، ورقه عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية ، السودان ٢٣–٢٥ أيلول ،٢٠٠١م ، ص ٦–٧

– مدحت رمضان :– جرائم الاعتداء على الأشخاص والإنترنت ، دار النهضة العربية ن القاهرة ،٢٠٠٧م ،ص ١٧.، وعلى مستوى الدول العربية فقد صدر عن مجلس وزراء العدل العرب بجامعة الدول العربية قانون عربي استرشادي لمكافحة جرائم التقنية انظمه المعلومات مكون من ٢٧ مادة للاسترشاد به عند سن القوانين غير أننا لم نر له أثرا فعليا علي أغلب التشريعات الجنائية في الدول العربية وبصفة خاصة مصر، فلا يوجد بها حتى الآن تشريع جنائي خاص بالجريمة الالكترونية يقدم الحلول الناجعة لكافة المشكلات القانونية الناجمة عنها على الرغم من وجود بعض النصوص القانونية التي تحتويها قوانين تنظم موضوعات مختلفة تناولت بعض صور التجريم الالكتروني ،منها قانون الأحوال المدنية المصري رقم ١٤٣ لسنة ١٩٩٤ ، قانون حماية الملكية الفكرية رقم ٨٢ لسنة ٢٠٠٢ ، قانون تنظيم الاتصالات ١٠ لسنة ٢٠٠٣، وقانون التوقيع الالكتروني ١٥ لسنة ٢٠٠٤، وقانون الطفل المعدل في ٢٠٠٨، إلا أن هذه القوانين لم تغط كافة صور التجريم الالكتروني راجع :– – قرار مجلس وزراء العدل العرب الدورة التاسعة القرار رقم ٤٩٥–د١٩– ٢٠٠٣/١٠/٨م ، ومجلس وزراء الداخلية العرب الدورة الحادية والعشرون القرار ٤١٧–د٢٠٠٤/٢١م راجع :– هدى حامد قشقوش :– حماية الحاسب الاليكتروني ، في التشريع المقارن ، دار النهضة العربية ، القاهرة ١٩٩٢م ، ص١٠٢–١٠٣.

قد يبدو ذلك الحل أمام الدول التي لم تشرع قوانين لتجريم مختلف الجرائم الناتجة عن الاستخدام غير المشروع لشبكة الإنترنت سوى تطبيق القوانين القائمة بموادها التقليدية على هذه الوقائع خوفا من إفلات الجناة من قبضة العدالة.

ولكن تطبيق هذه النصوص التقليدية بمفهومها الواسع والخاصة ببعض الجرائم مثل السرقة وتطبيقها على بعض الوقائع التي تحدث على الانترنت من شأنه المساس بمبدأ الشرعية الجنائية (**Nullum crimen, nulla poena sine lege**)وهو من المبادئ الدستورية ([٤٧])، إذا ترك الأمر بيد القضاء لتفسير النصوص القائمة على نحو أوسع من الذي وضعت لأجله .

<u>المشكلات المتعلقة بالاختصاص والقانون واجب التطبيق:-</u>

يطرح في هذا المجال تساؤلا نراه في غاية الأهمية : مدي استجابة القواعد التقليدية لتحديد نطاق تطبيق القانون من حيث المكان؟ وهل هناك تحديات مرتبطة بالاختصاص بنظر جرائم الاعتداء على أمن المعلومات ؟

بالنسبة للاختصاص بالنظر في الجريمة فإنه يلاحظ أن اختصاص القضاء بنظر الجرائم الإليكترونية والقانون الواجب تطبيقه على الفعل لا يحظى دائما بالقبول أو الوضوح أمام حقيقة أن أغلب هذه الأفعال ترتكب من خارج حدود الدولة بالنظر إلى طبيعة هذه الجريمة باعتبارها عابرة للحدود ،أو إنها تمر عبر شبكات معلومات وأنظمة خارج الحدود ، حتى عندما يرتكبها شخص داخل حدود دولة نفسها ، وهو ما يبرز أهمية اختبار مدى ملائمة قواعد الاختصاص والقانون الواجب التطبيق ، وما إذا كانت القواعد والنظريات في هذا المجال تطال هذه الجرائم ذات الطبيعة المتفردة، وما تثيره من إشكاليات فيما يخص الاختصاص القضائي.

ويرتبط بمشكلات الاختصاص وتطبيق القانون مشكلات الملاحقة والتحري ، والضبط والتفتيش خارج الحدود ، وما يحتاجه من تعاون دولي شامل للموازنة بين التزام المكافحة

---

٤٧ – حرص المشرع الدستوري المصري على النص عليه في المادة ٩٥ من الدستور المصري الحالي الصادر في عام ٢٠١٤

والسيادة الوطنية([٤٨]) ، ويفرض التنازع الإيجابي للاختصاص ضرورة إيجاد حلول مستحدثة وابتكار مفاهيم قانونية جديدة دون الإخلال بمبدأ الشرعية الجنائية.

وللتغلب على مشكلة تنازع الاختصاص الايجابي يوجد حلان الأول يتمثل في إعطاء الأولوية لأحد الدول المتنازعة وفقا لأحد قواعد الاختصاص المتعارف عليها ، ونرى أن أكثرها جدوى وفاعلية هو مبدأ الإقليمية.

أما الحل الثاني فيتمثل في تدعيم وتعزيز الملاحقة الجنائية في كل واقعة يخشى فيها إمكانية إفلات المتهم من العقاب([٤٩])

مشكلة تقادم الجريمة والعقوبة :-

يمثل نظام تقادم العقوبة والجرائم وسيلة لمرتكبي الجرائم والمحكوم عليهم للإفلات من الملاحقة أو تنفيذ الأحكام ، وقد أغفل القانون الحالي للتعامل مع جرائم تقنية المعلومات رقم ١٧٥لسنة٢٠١٨م القواعد المنظمة لتقادم الجريمة ، وفي هذا الأمر يجب اعتبار جرائم الاعتداء على أمن البيانات مرتكبة وقت ارتكاب السلوك ، أو وقت حدوث النتيجة الإجرامية ، أي اعتبار وقت ارتكاب السلوك أو وقت حدوث النتيجة الإجرامية نقطة بداية سريان نظام التقادم ، أو باعتبار بعض جرائم التعدي على أمن البيانات من قبيل الجرائم المستمرة بما يكفل مدة أطول للتقادم([٥٠])

ثانيا حجية الدليل الرقمي في القضاء الجنائي :-

إن_مجرد الحصول على الدليل الرقمي وتقديمه للقضاء لا يكفي للتعويل عليه كدليل للإدانة ، مناط ذلك غلى هذا الدليل يمكن العبث بمضمون ما يحرف حقيقته ، وبالتالي لا يكون إلا في قدرة المختص فقط إدراك ذلك العبث ، كما إن نسبة الخطأ في الحصول على دليل صادق في

---

[٤٨] – محمد شوابكة ، جرائم الحاسوب والإنترنت ، دار الثقافة عمان ، ط١، ٢٠٠٤ . ص ١٣.، وقد تلافى المشرع المصري في القانون رقم ١٧٥ لسنة ٢٠١٨م هذه المسألة في المادتين الثالثة والرابعة

[٤٩] – عبد الفتاح بيومي حجازي ، مرجع سابق ، ص ٦٦٥.

[٥٠] – خالد ممدوح إبراهيم ، الجرائم المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، ط١ ، ٢٠٠٩م ، ص ١٥٨.

الإخبار عن الحقيقة تبدو عالية في مثل هذا النوع من الأدلة ، وبالتالي تقوم فكرة الشك في مصداقيتها كأدلة الإثبات الجنائي.

فهل ذلك يعني استبعاده من أدلة الإثبات الجنائي لتعارضه وقرينة البراءة ؟ وفقا للنظام اللاتيني في الإثبات يمتلك القاضي سلطة واسعة في تقييم الدليل من حيث قيمته فله أن يقبله ، أو أن يطرحه ، ومرد ذلك كله بالطبع اقتناع القاضي به، إلا أن سلطة القاضي على ذا النحو لا يجب التوسع فيها لتشمل الأدلة العلمية ، فالقاضي بثقافته القانونية لا يمكنه إدراك الحقائق الموصلة بأصالة الدليل الرقمي ، فضلا عن ذلك فإن هذا الدليل يتمتع من حيث قوته الدلالية بقيمة إثباتيه تصل لحد اليقين شانه شأن الأدلة العلمية تماما متى توافرت فيه شروط اليقين فلا يمكن معه القبول بممارسة القاضي لسلطته في التأكد من ثبوت تلك الوقائع التي يعبر عنها هذا الدليل ، ولكن لا يتناقض مما سبق أن الدليل الرقمي يظل موضوع شك من حيث سلامته من العبث من ناحية ن وصحة الإجراءات المتبعة في الحصول عليه من ناحية أخرى ، حيث تشكك في سلامته من ناحيتين :-

الناحية الأولي :- الدليل الرقمي يمكن أن يخضع للعبث لخروجه على نحو يخالف الحقيقة ، فقد يقوم هذا الدليل معبرا عن واقعة معينه صنع لأجل التعبير عنها خلافا للحقيقة ، دون أن يكون في غير استطاعة غير المختص إدراك ذلك العبث ، على نحو يمكن معه القول أن ذلك قد أصبح هو الشأن السائد في نظر سائر الأدلة الرقمية المقدمة للقضاء ،حيث إن التقنية الحديثة يمكن العبث بالدليل الرقمي بسهولة ، وجعله يبدو كنسخة أصلية.

الناحية الثانية :- إن كانت نسبة الخطأ الفني في الحصول على الدليل الرقمي نادرة للغاية إلا أنها تظل ممكنة ، يرجع ذلك الخطأ في الحصول على الدليل الرقمي لسببين :-(ا)- الخطأ في استخدام الأداة المناسبة في الحصول على الدليل الرقمي ، ويرجع ذلك للخلل في الكود المستخدم ،أو بسبب استخدام مواصفات خاطئة.(ب)- الخطأ في استخلاص الدليل بسبب اتخاذ قرارات لاستخدام الأداة تقل نسبة صوابها عن١٠٠% يحدث بسبب وسائل اختزال البيانات ،أو بسبب معالجة البيانات بطريقة تختلف عن الطريقة الأصلية التي تم تطبيقها خلاصة القول أن السلطة في الدليل الرقمي لا يتعلق بمضمونه كدليل وإنما لعوامل مستقلة عنه متى توافرت مصداقيته.

الخاتمة

تعرضنا في دراستنا البحثية هذه والتي أرجو من المولى عز وجل أن يكون التوفيق قد حالفني فيها موضوعا نراه في الآونة الأخيرة احتل مكان الصدارة سواء على المستوى المحلي ، أو على الصعيد الدولي نظرا لتداعياته والأخطار الناجمة عنه ، وهو موضوع أمن المعلومات وسبل مواجهة الاعتداءات الواقعة عليه والكيفية التي يمكن بها حمايته نظرا للاعتماد المتزايد على المعلومات في البيئة الإليكترونية سواء على المستوى الشخصي أو الحكومي.

وفى الجز الأول من هذه الدراسة تعرضنا لتعريف ماهية أمن المعلومات والتحديات التي يواجهها في البيئة الاليكترونية. ، وأهم تصنيفات وأساليب التهديدات الأمنية.

وفي الجزء الثاني تناولنا المواجهة التقنية والتشريعية لحماية أمن المعلومات من الاعتداءات الواقعة عليه وإشكاليات ذلك ، والذي من خلاله تناولنا في بدايته إلى سبل المواجهة التقنية لحماية أمن المعلومات في البيئة الاليكترونية ، ثم عرجنا إلى الاتجاهات التشريعية لأمن النظام المعلومات ، ثم تناولنا دراسة الإطار الدولي لحماية أمن المعلومات ثم دراسة مقارنة لبعض التشريعات الدولية والإقليمية وموقف المشرع المصري ، وأخيرا مدى ملائمة كل ذلك لحماية أمن المعلومات ، وخلصنا في دراستنا هذه إلى بعض النتائج ، وما أفرزته الدراسة من بعض التوصيات ، وذلك على النحو التالي:-

أهم النتائج :-

- إن محل جرائم الاعتداء على المعلومات هو نظام المعلوماتية بمكوناته غير المادية، أما مكوناته المادية فالاعتداء عليها مجرم بنصوص التجريم التقليدية

-غياب نصوص ودولية موحدة تواجه جرائم العالم الافتراضي، وغياب نصوص دولية موحدة تكفل الحماية الجنائية على شبكة الإنترنت.

- إن هدف التدابير التشريعية و وسائل امن المعلومات ضمان توافر ثلاثة عناصر أساسية للمعلومات ونظم معالجتها هي :الاستئثار، الجدية ولسلامة.

– إن فكرة تطويع النصوص التقليدية وتعديلها بما يتلاءم وطبيعة البيئة المعلوماتية لا يحقق الحماية الكافية لأمن المعلومات للطبيعة المتطورة لهذه الجرائم ومن ثم يصبح البحث عن سبيل آخر أمرا لا مفر منه.

– أهم مميزات جرائم الاعتداء على نظم المعلوماتية هو استهدافها للمعلومات بأشكالها المتباينة في البيئة الإلكترونية وليست ذات الكيان مادي.

– وعلى ذلك فقد توصلنا إلى أن من أهم لدواعي هو تدخل المشرع لإصدار نصوص تحظر الاعتداء على نظم المعلوماتية في التشريع المصري القائمة على الإحاطة بكافة أشكال الاعتداءات التي تقع على مكوناتها غير المادية، خاصة مع العجز الذي كان يشوب التشريع في مواجهتها للجرائم التي كانت ستترتب عليه آثار خطيرة، نتيجة ارتكاب أفعال غير مشروعة ويفلت أصحابها من العقاب بسبب عدم وجود نصوص يجرمها ،وحسنا فعل المشرع المصري عندما أقر مشروع القانون الأخير لمكافحة هذه الجرائم.

–هناك بعض من العوائق التي تعيق مكافحة الاعتداءات الواقعة على أمن المعلومات في إطار البيئة الإليكترونية بعضها تشريعي وبعضها إجرائي هذه التعقيدات ناتجة عن طبيعية هذه الجريمة سواء من ناحية تطورها التقني ،أم من ناحية طبيعتها العابرة للحدود والآثار الخطيرة الناجمة عنها والتي قد تصيب العديد من البلدان في آن واحد.

<u>أهم التوصيات</u> :–

- ضرورة المراجعة الدورية للتشريعات الجزائية القائمة وإزالة أي غموض أو ثغرات من الممكن أن يستغلها الجناة للإفلات من العقاب.
- تعزيز التعاون الدولي في مكافحة الجرائم المعلوماتية ، بهدف التقريب بين القوانين الوطنية الجزائية ، وجمع الأدلة وتسليم المجرمين ، وتبادل الخبرات والمعلومات المتعلقة بهذا الأمر.
- إنشاء وحدات خاصة يناط بها مهمة التحري والتعمق في البيئة الإليكترونية سواء على المستوى الوطني أو الدولي على أن يتم بالتوازي الاهتمام بتدريب وإعداد الكوادر الشرطية المؤهلة للتعامل مع جرائم الاعتداء على المعلومات ذات الطبيعة التقنية المعقدة ، وتعزيز قدراتهم على التحقيق فيها وتأمين الأدلة التقنية.
- تمكين القضاة وأعضاء النيابة وإعدادهم لملاحقة ومقاضاة مرتكبي جرائم تقنية المعلومات والاستفادة من الأدلة التقنية من خلال التدريب والتخطيط.

- تدريس الجرائم التقنية وكل ما يخصها واعتبارها مادة أساسية في المعاهد الأمنية ومؤسسات إعداد القضاة ومناهج الدراسة الخاصة بالقانون الجنائي لتخريج كوادر قادرة على التعامل مع مثل هذه الاعتداءات والجرائم.
- يجب أن تتضمن مقومات واستراتيجيات مواجهة جرائم الاعتداء على المعلومات ومحاربتها بجانب القوانين الجنائية الموضوعية قوانين إجرائية تتماشى وطبيعة البيئة الرقمية ، وبخاصة مسألة استخلاص الدليل الرقمي بدون المساس بحقوق الإنسان وحرياته الأساسية وتعريضها للخطر ولذلك قيل بأن من يتقن وضع قانون عقوبات ثم يترك قانون الإجراءات الجنائية بدون إتقان كمن يبني قصرا في الهواء.
- ضرورة الاتفاق من خلال تعزيز التعاون الدولي بالاتفاقيات الثنائية والمتعددة لمواجهه هذه الظاهرة الإجرامية ذات الطبيعة العابرة للحدود على حل جميع العقبات التي تحول دون ملاحقة مرتكبي هذه الجرائم ، وبخاصة مشاكل تنازع الاختصاص وتسليم المجرمين
- النص في القانون المصري الجديد على تقادم العقوبة في هذه النوعية من الجرائم واعتبارها من الجرائم المستمرة في سريان مدة التقادم للتقليل من الإفلات من العقاب
- استحداث نص خاص بالتزوير المعلوماتي ، وتوسيع مفهوم المحرر ليشمل أية دعامة أخرى.

قائمة المراجع

أولا المراجع العربية :-

- **أحمد فتحي سرور** :- الحق في الحياة الخاصة ، مجلة القانون والاقتصاد للبحوث القانونية والاقتصادية ، مطبعة جامعة القاهرة ، العدد٥٤، ١٩٨٦م.
- **آدم عبد البديع آدم حسين** :-الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها له القانون الجنائي ، رسالة دكتوراه ،كلية الحقوق ، جامعة القاهرة ،٢٠٠٠م .
- **أسامة عبد الله قايد** :- الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، بدون دار نشر ورقم طبعة ، ١٩٨٠م.
- **أشرف شمس الدين** ، الحماية الجنائية للمستند الإليكتروني ، ط١ ، دار النهضة العربية ، القاهرة ، ٢٠٠٦م.
- **أشرف صلاح الدين** ، طرق الحماية التكنولوجية بأنواعها وأشكالها المختلفة ، ورشة عمل بعنوان أمن وحماية نظم المعلومات في المؤسسات العربية ، القاهرة ، ٢٠٠٧.
- **إيهاب ماهر السمباطي** :-الجرائم الإليكترونية والجرائم السيبرية وظيفة جديدة ، فئة مختلفة ، التناغم القانوني هو السبيل الوحيد ، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر ، المغرب ١٩-٢٠ يونيه ٢٠٠٧، م.
- **جلاد سليم** :- الحق في الخصوصية بين الضمانات والضوابط في التشريع الجزائري والفقه الإسلامي ، رسالة ماجستير ، كلية العلوم الإنسانية والحضارة الإسلامية ، جامعة وهران ، الجزائر ٢٠١٣-٢٠١٤م.
- **جميل زكريا محمود** ، الفيروسات وطرق الوقاية منها كوسيلة لأمن البيانات ، المؤتمر الدولي الأول حول أمن المعلومات ، نحو تكامل رقمي آمن ،١٨-٢٠ ديسمبر٢٠٠٥م ، مسقط عمان .
- **حسن طاهر داوود** ، الحاسب وامن المعلومات ، مركز الدراسات و البحوث ، المملكة العربية السعودية ، ٢٠٠٠م.
- **خالد ممدوح إبراهيم** ، الجرائم المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، ط١ ، ٢٠٠٩م.
- امن المعلومات الالكترونية ، الدار الجامعية ، القاهرة ،٢٠٠٨م.
- **ذيب بن عايض القحطاني** ، أمن المعلومات ، مدينة الملك عبد العزيز للعلوم التقنية ، الرياض ١٤٣٦هـ - ٢٠١٥م.
- **سعد غالب ياسين** ، نظم المعلومات الإدارية الطبعة العربية ،دار اليازوري العلمية للنشر والتوزيع ، عمان الأردن ،٢٠٠٩م.
- **عائشة بن قارة مصطفي** :- حجية الدليل الإليكتروني في مجال الإثبات الجنائي ، دار الجامعة الجديدة الإسكندرية ،٢٠٠٩م.

- **عبد الجبار الحنيص** :- الاستخدام غير المشروع لنظام الحاسوب من وجهة نظر القانون الجزائي " دراسة مقارنة" ، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية ، المجلد٢٧ ، العدد الأول ، ٢٠١١م.
- **عبد العظيم مرسي وزير**: شرح قانون العقوبات ، دار النهضة العربية.
- **عبد الفتاح بيومي حجازي**،التجارة الإليكترونية وحمايتها القانونية ، دار الفكر الجامعي ، الإسكندرية ،٢٠٠٤م.
- **عبد المحسن بدوي محمد أحمد** :- إستراتيجيات ونظريات معالجة قضايا الجريمة والانحراف في وسائل الإعلام الجماهيرية ، الندوة العلمية حول الإعلام والأمن ، مركز الدراسات والبحوث ، قسم الندوات واللقاءات العلمية ، أكاديمية نايف العربية للعلوم الأمنية ،١١-١٣ /٥ /٢٠٠٥م.
- **عفيفي كامل عفيفي** ، جرائم الكمبيوتر ودور الشرطة والقضاء ، رسالة دكتوراه ، كلية الحقوق ، جامعة الإسكندرية ، ١٩٩٩م.
- **علي محمود علي حمودة** :- الأدلة المتحصلة من الوسائل الإليكترونية في إطار نظرية الإثبات الجنائي ، مقدم للمؤتمر العلمي الأول حول الجوانب القانونية الأمنية للعمليات الإليكترونية ، أكاديمية شرطة دبي ، ٢٨-٢٠٠٣/٤/٢٩م.
- **عوض الحاج على أحمد** ، عبد الأمير خلف حسين ، أمنية المعلومات وتقنيات التشفير ، دار الحامد للنشر والتوزيع ، الأردن ،٢٠٠٠م.
- **غنام محمد غنام** ، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر ، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت ، الإمارات العربية المتحدة ، كلية الشريعة والقانون ، ١-٣مايو ٢٠٠٣م ، المجلد الثاني.
- **فاطمة مرينز**:- الاعتداء على الحق في الحياة الخاصة عبر شبكة الإنترنت ، رسالة دكتوراه ، جامعة أبو بكر بلقان ، تلمسان ، الجزائر ،٢٠١٢-٢٠١٣م .
- **قانون الأونيسترال** النموذجي للتوثيق التجاري الدولي مع دليل الاشتراع استعماله ، منشورات الأمم المتحدة ،. ٢٠٠٤ .A05.V4.
- **القانون رقم ١٧٥** لسنة٢٠١٨م في شأن مكافحة جرائم تقنية المعلومات المنشور بالجريدة الرسمية العدد٣٢ مكرر في١٥ أغسطس ٢٠١٨.
- **قرار مجلس وزراء** العدل العرب الدورة التاسعة القرار رقم ٤٩٥-د١٩- ٢٠٠٣/١٠/٨م.
- **محمد أبوبكر يونس** ، الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية والجوانب الإجرائية ، دار الثقافة العربية للنشر ، ٢٠٠٤م.
- **محمد بن عبد الله القحطاني** ، امن المعلومات ، جامعة الملك عبد العزيز للعلوم والتقنية , الرياض ،٢٠٠٩م.
- **محمد حماد مرهج الهيتي**، "جرائم الحاسوب" ، ١ط ، إدارة المناهج للنشر والتوزيع ، عمان، ٢٠٠٦م .

- **محمد شوابكة** ، جرائم الحاسوب والإنترنت ، دار الثقافة عمان ، ط١، ٢٠٠٤ . ص ١٣.، وقد تلافى المشرع المصري في القانون رقم ١٧٥ لسنة ٢٠١٨م.
- **محمد فهمي طلبة** ، فيروسات الحاسب وأمن البيانات ،مجموعة النيل العربية للطباعة والنشر ،١٩٩١م.
- **محمد محمد الألفي** ، ورقة عمل مقدمة في ندوة حماية نظم المعلومات في المؤسسات العربية ، القاهرة ، ٢٠٠٧م.

- **مدحت رمضان** :- جرائم الاعتداء على الأشخاص والإنترنت ، دار النهضة العربية ن القاهرة ،٢٠٠٧م.
- **مفتاح بو بكر المطردي** ، الجريمة الإليكترونية ، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية ، السودان٢٣-٢٥ أيلول ٢٠٠١م.
- **ممدوح الشحات صقر** ، ورقة عمل مقدمة في ندوة حماية نظم المعلومات في المؤسسات العربية ، القاهرة ، ٢٠٠٧م.
- **ممدوح خليل بحر** :- نطاق حماية الحياة الخاصة في القانون الجنائي ، دار الثقافة للنشر والتوزيع ، الأردن ، ٢٠٠٦م.
- **ممدوح عبد الحميد عبد المطلب** ، زبيدة محمد قاسم ، عبد الله عبد العزيز، أنموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر ، مؤتمر الأعمال المصرفية الإليكترونية ، كلية الشريعة والقانون ، الإمارات ، غرفة تجارة وصناعة دبي، ٥-٢٠٠٣/١٢/١٠م.

- **نادية أمين محمد علي** ، الفيروسات وطرق الوقاية منها كوسيلة لأمن البيانات ، المؤتمر الدولي الأول حول أمن المعلومات ، نحو تكامل رقمي آمن ، ١٨-٢٠ ديسمبر ٢٠٠٥ ، مسقط عمان.
- **نائل عبد الرحمان صالح** ،واقع جرائم الحاسب في التشريع الأردني ، بحيث مقدم لمؤتمر القانون والكمبيوتر والانترنت الذي نظمته كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة) 2000 (بحوث مؤتمر القانون والكمبيوتر والإنترنت ، المجلد الأول ، الطبعة الثالثة ، كلية الشريعة والقانون جامعة(الإمارات العربية المتحدة ، ٢٠٠٤م.
- **نائلة عادل محمد فريد قورة**، جرائم الحاسب الاقتصادية، رسالة دكتوراه، جامعة القاهرة، كلية الحقوق، طبعة ٢٠٠٣م.
- **نجم عبد الله الحميدي** ، نظم المعلومات الإدارية مدخل معاصر ، الطبعة الثانية ، دار اليازوري للنشر والتوزيع, عمان ، الأردن ، ٢٠٠٩م.

- **نظام مكافحة جرائم المعلوماتية** ، هيئة الاتصالات وتقنية المعلومات ، المملكة العربية السعودية .
- **هدى حامد قشقوش** :- حماية الحاسب الاليكتروني ، في التشريع المقارن ، دار النهضة العربية ، القاهرة ١٩٩٢م.
- **هشام فريد رستم**، قانون العقوبات ومخاطر تقنية المعلومات،مكتبة الآلات الحديثة،أسيوط،١٩٩٢.
- الحماية الجنائية للإنسان في صورته ، مكتبة الآلات الحديثة ، أسيوط.

- **هيثم حمود الشبلي** ، إدارة مخاطر الاحتيال في قطاع الاتصالات ، دار صفاء للنشر والتوزيع ، ط١ ، عمان ، الأردن ٢٠٠٩م.
- **هيثم محمد الزعبي** ، إيمان فاضل السامرائي ، نظم المعلومات الإدارية ، الطبعة الأولى ، دار صفاء للنشر والتوزيع ، عمان ، ٢٠٠٤م .
- **وائل بندق** ، موسوعة القانون الإليكتروني وتكنولوجيا الاتصال والمعلومات ، دار المطبوعات الجامعية ، الإسكندرية ، ط١ ، ٢٠٠٧م.
- **يوسف خليل يوسف عبد الجابر** ، مدى فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإليكترونية في الشركات الصناعية الأردنية ، رسالة ماجستير ، جامعة الشرق الأوسط ،٢٠١٣م.
- **يونس عرب** :- قراءة في الاتجاهات التشريعية للجرائم الإليكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان ، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإليكترونية ، مسقط ، ٢-٤ أبريل ٢٠٠١م.
- **يونس عرب** ، جرائم الكومبيوتر والانترنت ، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات ، ورقة عمل مقدمة إلى مؤتمر الأمن العربي ٢٠٠٢م تنظيم المركز العربي للدراسات والبحوث الجنائية ، أبو ظبي ، ص١١ ، ١٠/ -١٢/٢ ٢٠م.

ثانيا المراجع الأجنبية:-

- **Manish Gupta and Raj Sharman** , Social and Organizational Liabilities in Information Security , publishing Information Science Reference , Hershey , New York , 2009 .P.296
- **Micki Krause ; Harold F. Tipto**n , Information Security Management Hand book , Sixth Edition , Auerbach Publication , New York , 2008.
- **Romney , M& Steinbart ,P.** , Accounting information's system ,12ed., ENGLAND. Pearson education,2012.
- **Samuel D. Warren &Louis D. Brandeis** , The right of piracy , Harvard law review , Vol. IV., Dec. 15, 183-220
- **Todd G. Shipley, Henory R. Reev**e, Collecting evidence from a running computer , The national consortium for justice information and statistic ,2006